Deloitte.

Secure by Design: A CISO's guide to a practical approach

Contents

Build your foundational security program to support a scalable Secure by Design approach

The role of the chief information security officer (CISO) has become increasingly complex due to the rapid changes and growth typically seen in the technology landscape. To keep up with this pace, it is important for CISOs to gain visibility into how systems are being secured before they are released into production. Achieving this visibility calls for a structured Secure by Design approach, which means that security is integrated into each stage of the development process, from initial design to final deployment. This approach not only helps in identifying and mitigating potential security risks early on but also establishes that security measures are consistently applied across projects.

Secure by Design: Deloitte's perspective

"Secure by design" has recently become a popular DevSecOps principle. It focuses on shifting security as far left as possible in the development process. Secure by Design has led teams to prioritize security considerations early in the application design process rather than just before deployment.

This principle has been introduced to help organizations address cyber vulnerabilities and bolster their cybersecurity defenses. Using a "secure by design" approach allows organizations to proactively identify and mitigate potential risks. This approach not only facilitates consistent application of security controls but also supports alignment with industry standards and regulatory requirements. Additionally, it offers a cost-effective solution by reducing the need for expensive security fixes later in the development life cycle.

Foundations of Secure by Design

To begin evaluating security in the early stages of development, it is important to establish a standardized approach. This approach should clearly define the types of reviews to be conducted, the controls to be implemented, and the required level of verification. By doing so, you can be confident that security measures are consistently applied throughout the development life cycle, enabling a proactive Secure by Design strategy. Additionally, it is essential to make security efficient and not a burden on the development process.

Secure by Design components

When designing a Secure by Design program, begin by defining the core foundational components. These should include:

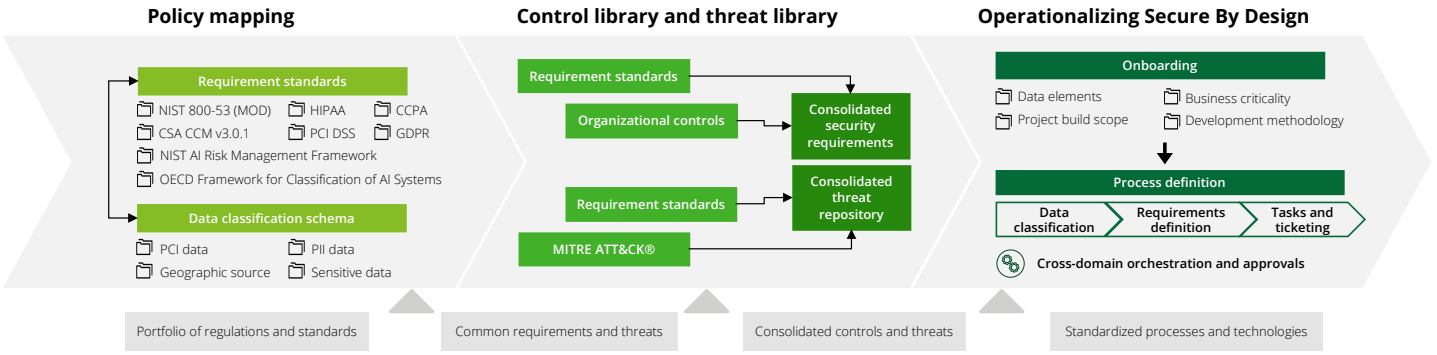
1. Establishing a Common Controls Framework (CCF)
2. Policy mapping from the CCF to policy directives
3. Creating a policy gap analysis
4. Designing an end-to-end process flow, including workflows for multiple use cases
5. Understanding your asset portfolio to maintain visibility into your organization's risk landscape

The core components of Secure by Design aim to help address challenges that a CISO organization may encounter. Often, organizations begin implementing a shift-left solution as part of an individual project or technology shift without considering foundational prerequisites disassociated from a specific technology. Using cloud migration as an example, many organizations build specific workflows, review boards, and approval criteria based on the need to shift to the cloud. Later, it becomes very difficult to scale the program effectively without intensive remediation efforts. With Secure by Design focused on reviewing cloud components only, the process and framework used cannot scale effectively to include new technologies such as artificial intelligence (AI). Thus, we recommend a standard framework and approach that reviews each application of new technology broadly. As technology advances, adding cloud or AI review components becomes a bolt-on and not a whole new approach.

Establishing a Common Controls Framework

Defining a framework and operationalizing Secure by Design

Any organization whose security policies are derived from cybersecurity standards such as NIST 800-53, CSA CCM, PCI DSS, HIPAA, GDPR, or CCPA should be mapped to control libraries. These standardized controls can be used to conduct security operations such as reviews, scans, and vulnerability management.



National Institute of Standards and Technology (NIST), Health Insurance Portability and Accountability Act (HIPAA), California Consumer Privacy Act (CCPA), Cloud Security Alliance Cloud Controls Matrix (CSA CCM), Payment Card Industry Data Security Standard (PCI DSS), General Data Protection Regulation (GDPR), Personally Identifiable Information (PII), Organization for Economic Co-operation and Development (OECD).

Before building an automated solution to enforce the Secure by Design approach, it's important that organizations have clearly defined policies and a detailed controls library. The controls library is typically referred to as the CCF and may be based on one or more industry standard frameworks or regulatory requirements—for example, Control Objectives for Information and Related Technologies (COBIT), NIST, International Organization for Standardization/ International Electrotechnical Commission (ISO/IEC) 27001, ISO/IEC 8183:2023, PCI DSS, HIPAA, and OECD Framework for the Classification of AI Systems. A CCF should represent the extensive set of possible security and privacy controls that may be applied to a project. It provides a foundation to automate control assignment based on granular project criteria such as data classification, hosting location, or asset type.

Many organizations face challenges consistently applying security controls across projects. This can be due to disparate controls frameworks, a lack of policy-driven controls, or asset types without defined control requirements. A CCF is essential to enforce a standardized approach to assigning, implementing, and assessing security controls.

Policy mapping

Secure by Design operationalizes policy-driven requirements enforcement, which can encourage better compliance with policy and show a traceable implementation of policy at a granular level.

To effectively operationalize a CCF for Secure by Design, an organization should possess a deep understanding of its policies and the implementation of security controls in alignment with those policies, and it should be able to document that understanding in a granular mapping of policies, requirements, and controls.

For example, a policy may dictate a requirement that penetration testing be conducted for an application with a data classification of "high" or above. Once the data classification is determined, security requirements are automatically generated based on the mapping that indicates the list of controls required for an application with a "high" data classification. This automated requirement assignment is powered by a precise policy mapping of security policies and standards to each control listed in the CCF. During later stages of development, and after deployment, policies should specify the required remediation actions for defects and vulnerabilities. Based on the business criticality of the application, the policy may mandate that critical and high vulnerabilities be addressed prior to release.

Creating a policy gap analysis

Once the CCF is developed and the organization's policies have been mapped to the CCF, a policy gap analysis can be conducted. This analysis identifies and addresses discrepancies between existing security policies and the CCF. For each control in the CCF, there should be policies tied to the control. Once policy gaps have been identified, the organization should create the additional policies required and map them to the CCF. Conducting a policy gap analysis allows organizations to confirm that their controls are relevant to regulations, industry standards, and leading practices. Systematically identifying and addressing policy gaps can help enhance the security posture of an organization and provide compliance with relevant regulations.

Designing an end-to-end process flow

Defining the process

When building an end-to-end Secure by Design process flow, identify the teams involved in an overall project life cycle, including but not limited to security-related groups—for example, data security; privacy; vendor risk; vulnerability management; security architecture; and governance, risk, and compliance (GRC). Each team will be responsible for certain activities at different stages of the development life cycle. These activities will be defined during the intake stage but will only be initiated and assigned at the appropriate stage.

The CCF is the foundation for a standardized review. During the process, each security domain will output criteria that were predefined in the CCF.

It is recommended that a centralized intake be created for users to initiate the Secure by Design process. The intake should include information about the project scope, business unit, business criticality, and intended function. This intake can stand alone or be triggered as part of a configuration management database (CMDB) to reflect how an organization tracks and manages assets.

The Secure by Design process includes a governance layer that enforces the defined end-to-end criteria based on the inherent risk calculation determined during the intake. Activities such as architecture reviews, threat modeling, data classification, and vulnerability testing are defined and enforced in the governance layer. Each one of these activities has its own process with its own criteria and output. As part of the Secure by Design solution, you can either orchestrate the tasks within each process in the governance layer or through integrations. With either method, the outputs will be returned to the governance layer for tracking and consolidation.

Below are some examples of tasks and stakeholder intake teams that may be included in the Secure by Design process:

Data security reviews the project's data classification and identifies whether it is consuming personal, financial, or health care data. The data classification then drives the security controls and confirms that they are compliant with regulatory requirements (e.g., PCI DSS, HIPAA).

Privacy confirms that the data consumed in the project follows both the organizational and regulatory security requirements applicable for working with sensitive data. Privacy determines the minimum amount of sensitive data required for the project to function, and a privacy impact assessment (PIA) is conducted to evaluate the potential privacy risks for the project.

Vendor risk assesses risk pertaining to third-party vendors that provide software, services, or components that are integrated into the project. This makes sure that the organization has clear contractual agreements with vendors that include security and privacy requirements. When the project is being developed, the third-party components should be securely integrated with the software including applicable security controls and code reviews aligned with the CCF controls that were generated for the project.

The Secure by Design process will also overlay the organization's software development life cycle (SDLC). At a single point in time, a project will undergo an end-to-end Secure by Design review, but as new features are released, previous applications of security controls are considered and re-reviews are conducted based on defined cadence/criteria (i.e., time-based, risk-based).

Designing a user-friendly solution

Creating a user-friendly solution is crucial because it allows end users to easily navigate and utilize the system, leading to increased productivity and a better user experience. A well-designed user interface and process can significantly reduce the learning curve, reduce errors, and enhance the overall user experience. When designing a user-friendly solution, it is essential to consider the number of meetings and handoffs required, as these can affect the efficiency and clarity of communication among team members. Keeping the user experience in mind throughout the development process helps to build a solution that is intuitive, accessible, and effectively addresses user requirements.

In developing a Secure by Design solution, it is essential to identify and involve various user personas, including business sponsors, project managers, application developers, risk management, security architects, and data privacy and security teams.

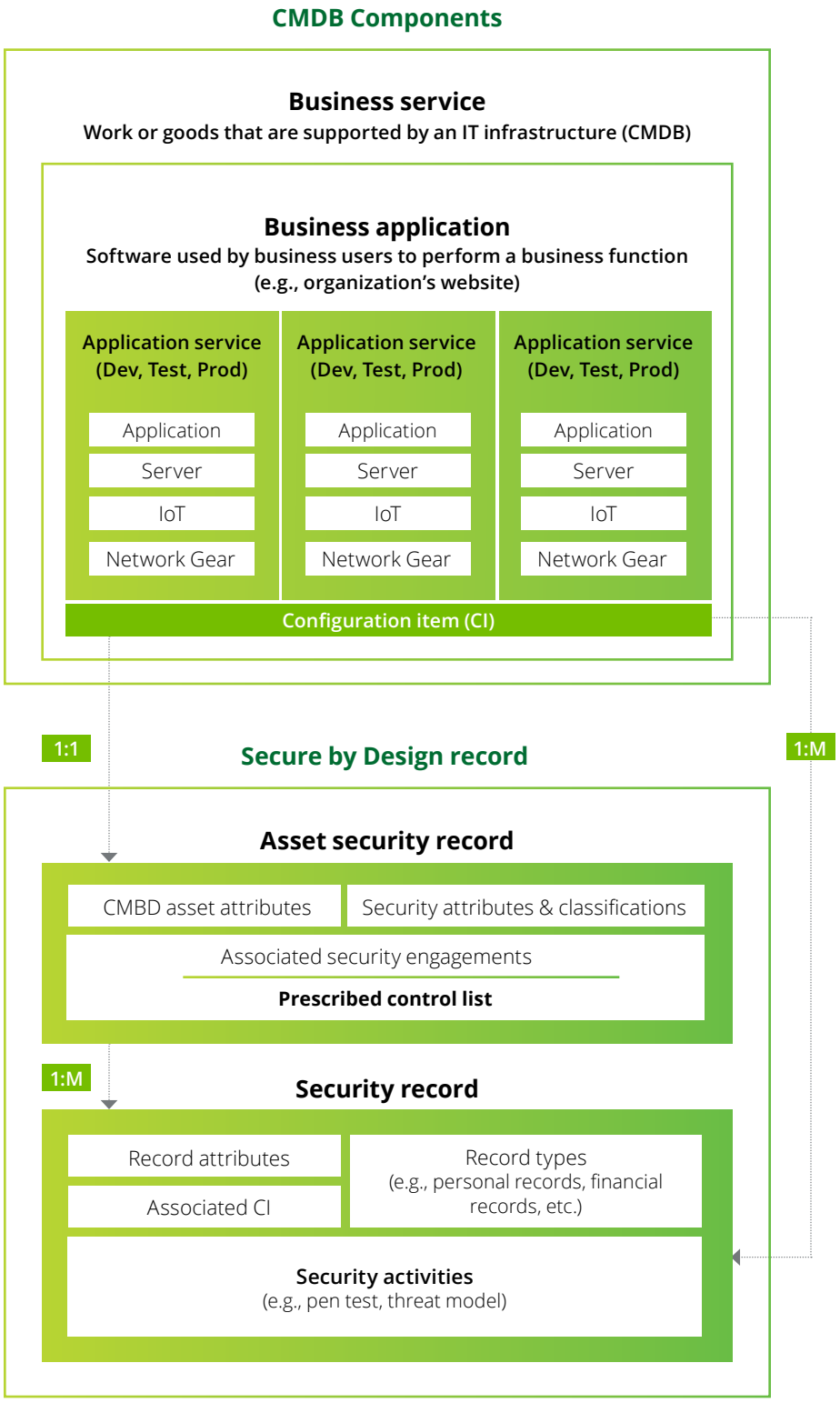
This process entails creating a unified orchestration platform that functions as a security portal, offering views customized for each persona. Each user persona should have a dedicated group within this platform with roles specifically assigned to them. Furthermore, the platform should incorporate persona-based dashboards that provide the project status and information tailored to each group's requirements. It is crucial to streamline tasks, assessments, and approvals to make them easy to accomplish, thereby supporting rather than disrupting daily business operations.

Understanding your asset portfolio

A security record structure should align with a CMDB. Many organizations face a challenge in understanding "what's out there"—highlighting the importance of maintaining visibility into your asset portfolio. Integrating Secure by Design with the CMDB offers visibility into the asset portfolio and security status at various levels. This integration is crucial for scalability, promoting governance and enforcement of security requirements across assets.

To build an effective end-to-end Secure by Design process, tie security records to the CMDB, which centralizes IT environment information. Security records should follow an asset structure linked to a business service level, encompassing IT-supported work or goods, and then to a business application, which acts as the parent record. Implement an application portfolio management (APM) approach to inventory applications, detailing their purpose, usage, and criticality. This visibility is important for understanding the security landscape and prioritizing efforts.

Integrating the CMDB with an orchestration platform automates security tasks, prescribes controls, and applies policies using standardized data. This integration enhances visibility, aids in identifying security risks, and aligns security measures with asset information. It facilitates consistent enforcement through automated workflows, continuous compliance monitoring, improved incident response, and streamlined change management, thus maintaining a strong security posture and supporting business goals.



Implementing task orchestration and enforcement

Beginning with a consolidated intake form, critical project information is collected and used to automate the generation of security tasks, the assignment of security assessments, the confirmation of security requirements, and approval for release.

Tasks should be determined by business criticality and risk. Policies define an overarching governance process that is essential to understanding and defining the tasks required in the project life cycle.

Secure by Design is powered by an underlying orchestration and governance platform that hosts the intake form and tasks and enables reporting and metrics. The solution includes a governance workflow that branches out to individual requirement workflows. Integration with tools and ticketing platforms enables automation and feedback loops. Centralized tasks, requirements, and policy tracking create a clear picture of compliance status.

Orchestration

Secure by Design process flows can be built on an orchestration platform to automate and manage tasks in a central location. A benefit of hosting your end-to-end security accreditation workflow in a single platform is the integration of multiple other security capabilities to read and write data to and from a single source of truth. Integrated security capabilities can include:

AI security

Identity and Access Management (IAM)

Application security

Infrastructure/ cloud/container

Data privacy

Security pattern development

GRC

Vulnerability management

Task assignment and enforcement

Foundations of Secure by Design

Secure by Design consists of several key workflows that occur throughout the Secure Software Development Life Cycle (SSDLC) process and across multiple business teams, and leverages automation to generate and assign security tasks and prescribe security controls based on one form completed by the customer.

Application security | **Risk management** | **Security architects** | **Data privacy** | **Cloud security** | **Vulnerability management**

Iterative process to align with Agile development

Intake
Secure by Design leverages a standardized intake form for security domains to identify the scope, risk, and project requirements. A security record is created to track pre-production security activities and outcomes throughout the project's life cycle.

Task creation
Tasks are created across multiple security teams and should be prioritized based on risk. Tasks should be centrally managed to enable transparency across security teams and tracking of the project's security record. Security teams include data security, privacy, vendor risk, application security, and security architecture.

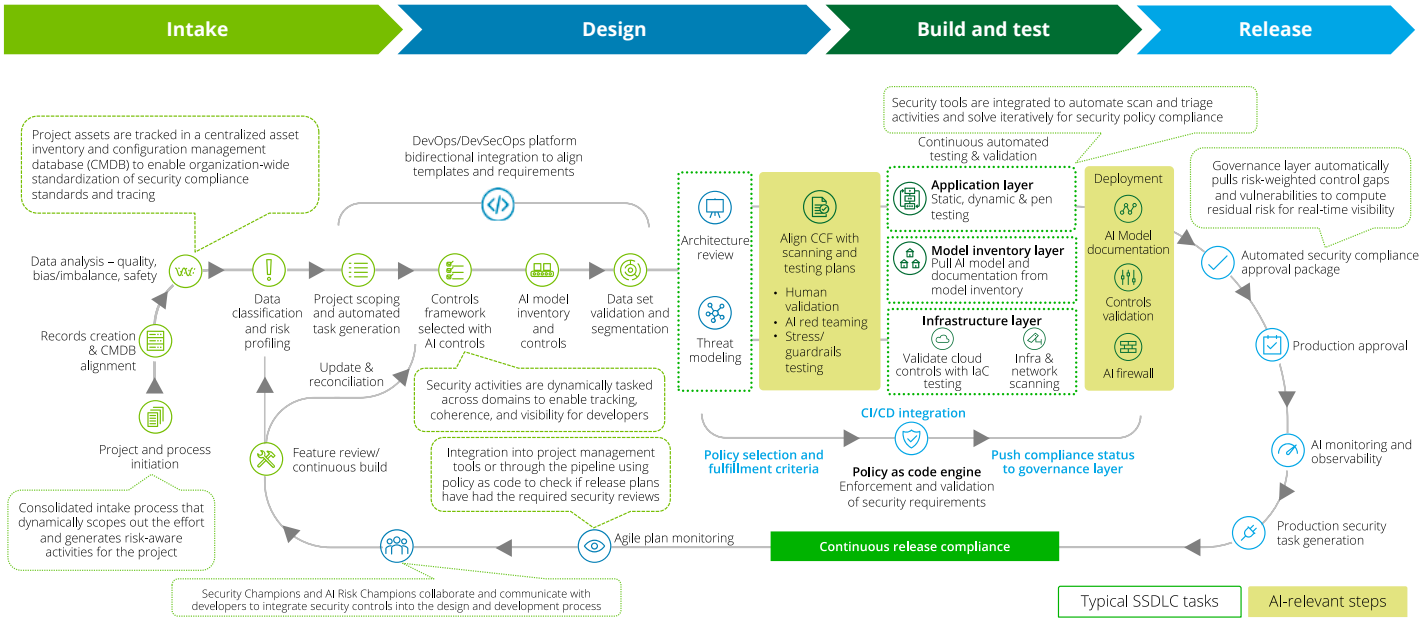
Security assessments
These assessments should be standardized and mapped to a defined control library or CCF. Utilizing security assessments allows the project team to provide additional information regarding their technical solution. As project teams respond to the assessments, controls are applied to the project record based on its scope. Example assessments include security architecture review, threat modeling, data security and privacy review, vulnerability testing, and vendor risk.

Security validation
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 automatically review overall compliance and reduce user error while confirming security controls.

Approval for release
Approval is granted for release after security teams review and confirm the implemented security controls against requirements defined for the project record during the Secure by Design life cycle. Approvals should be manually enforced through review boards/tollgates and automated in deployment pipelines. Evidence requirements are determined for security policies based on the organization's compliance requirements. Authority to Operate (ATO) can be automatically generated when the project is ready for release to indicate that the security controls comply with policies and have been confirmed before the project is released to production. A production security task can be implemented to provide continuous enforcement of security policies and controls, monitor access, and respond to potential threats.

Secure by Design workflow

The following workflow depicts an ideal and mature approach to achieving end-to-end security across the IT life cycle from the planning and ideation phase to the production state and beyond. It is powered by an automated governance and accountability layer to maintain security policy compliance throughout.



Integration

Leveraging a central orchestration platform to automate security tasks and assessment provides organizations with a single location to view their security posture. To further automate security activities in the security accreditation workflow, integrate the orchestration platform with application security testing tools, project management tools, issue tracking tools, etc.

Integrating additional systems and tools is fundamental to the effectiveness of Secure by Design. It enables centralized management, automation, enhanced visibility, improved incident response, streamlined change management, compliance, and governance. Organizations can leverage integrated tools to automate application security scanning tasks and activities to reduce the effort required from security teams. Leveraging project management tools and integrating them with the orchestration platform is essential for enhancing the visibility and effectiveness of managing IT operations. When an incident occurs, integration with project management tools enables teams to track the incident and link it to other relevant security activities, which can lead to faster resolution and better tracking of incident response efforts. Whenever a system requires a review for compliance or to evaluate root cause analysis, a clear history of activities is available.

An orchestration platform automates policy checks; feeds information to other tasks; and boosts efficiency by integrating diverse systems, tools, and processes. For instance, a threat model's output can automatically assign testing scenarios to penetration testing teams or monitoring cases to your security information and event management platform. This approach is designed to enhance operational efficiency and strengthen IT security and resilience.

Enabling visibility with dashboards and reporting

Given the centralized nature of the orchestration platform, Secure by Design enables dashboarding and reporting capabilities. Reporting is often considered later, but with the Secure by Design approach, these functionalities are enabled when the solution is built to provide early and consistent insight into the security posture of the organization, as well as an enterprise-wide view of the status of security requirements in IT projects across the organization.

Broad metrics

With Secure by Design dashboards enabled, organizations can track specific security program metrics, including:

- Overall project compliance
- Vulnerability remediation
- Current release security requirements status
- Backlog status and risk
- Control implementation status
- Team service level agreements (SLAs) and capacity

Operationalizing Secure by Design

Scaling Secure by Design

Scaling Secure by Design involves strategically enhancing the capacity and efficiency of security processes to manage increasing workloads and backlogs effectively. With clearly defined security tasks and requirements integrated into the development life cycle, project teams should expect additional work in their backlogs. To address the surge in work, additional resources can be brought on to clear existing backlogs while new work continues to accumulate. Backlog rationalization helps prioritize tasks based on risk and impact to address critical issues promptly.

Continuous enhancements will be needed to meet demand and scale efficiently. Opportunities for further automation will arise as processes develop and tasks become repetitive. Additionally, as the solution becomes standardized, patterns and blueprints can be established to expedite the development and review process. Automating routine business tasks enhances efficiency and reduces the workload for both project and security teams. This allows teams to concentrate on higher-value activities while maintaining security as an integral part of the development life cycle.

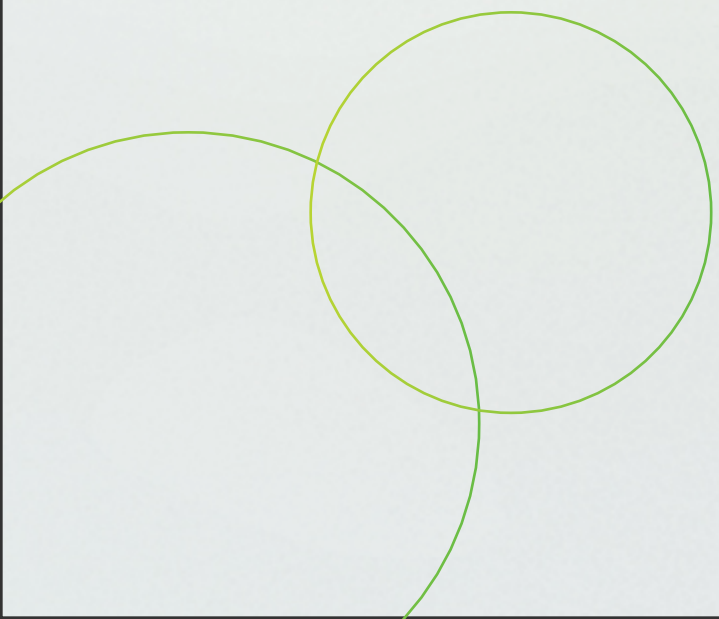
Enabling your teams to use Secure by Design effectively

To effectively implement Secure by Design, organizations should consider adopting a security-first culture; building a process that provides a positive end-user experience; socializing the process iteratively during the build and prioritizing feedback; providing training sessions and office hours to assist users as they begin to use the solution; and continuously looking for automation and process enhancements.

Conduct regular training sessions to educate teams about the importance of security and their role in maintaining it. Include training sessions about the orchestration platform, security tasks, and security policies that are implemented in the Secure by Design solution, and tailor training to teams and their specific security tasks or activities. Encourage a mindset where security is everyone's responsibility, not just the security teams'.

Document the Secure by Design workflow and additional processes for security tasks and assessments. Track each team's tasks, assessments, and processes as part of the Secure by Design workflow. Make this information easy to understand and access. Tooltips, walk-throughs, visuals, and other techniques should be used to avoid users referring to a large document.

Conduct a continuous feedback loop to improve security practices, security reviews, and assessments. Monitor security metrics such as the number of vulnerabilities detected, time to remediation, and compliance with security policies. Use these metrics to measure the effectiveness of the Secure by Design solution. Provide regular reports to stakeholders on the state of security, highlighting achievements, areas for improvement, and ongoing initiatives.



Why Secure by Design

Secure by Design can provide many differentiators to clients, including:

- **Ubiquity and agility:** Secure by Design integrates security into the end-to-end development process, making it an efficient part of the workflow.
- **Consumable security:** It simplifies security for the business, making it more accessible and easier to manage.
- **Centralized visibility and standardization:** Secure by Design enables centralized visibility and standardization of security requirements, facilitating consistent security controls and measures throughout the product life cycle.
- **Automation and orchestration:** The solution leverages automation to orchestrate multiple security tasks across teams involved in the project life cycle. This includes automated requirements tracking, task assignment, and updates in a central platform.
- **Integrated security capabilities:** Secure by Design integrates various security capabilities, such as data privacy, application security, risk management, vulnerability management, and cloud security into the SDLC.
- **Enhanced efficiency:** By reducing latency and redundancy, Secure by Design enables automated operations, increasing overall efficiency.
- **Cross-domain orchestration:** It provides tasking and tracking across various security departments and personnel, facilitating clarity of task and approval status through each developmental tollgate.
- **Real-time visibility:** The governance layer automatically pulls risk-weighted control gaps and vulnerabilities to compute residual risk for real-time visibility.

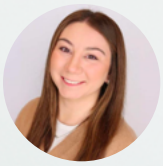
These differentiators make Secure by Design a broad and efficient solution for integrating security into the development process, making sure that security is not a burden but rather a natural part of the workflow.

Learn how to harness the power of Secure by Design here.

Authors

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

Ayla Hitchcock
Senior Consultant
Secure by Design Professional
Deloitte & Touche LLP
aylahitchcock@deloitte.com



Jasmine Baker
Consultant
Secure by Design Professional
Deloitte & Touche LLP
jasbaker@deloitte.com

Contacts

Contact our team to learn more about Secure by Design.

Adnan Amjad
Partner
US Cyber Leader
Deloitte & Touche LLP
aamjad@deloitte.com

Kevin Heckel
Managing Director
US Enterprise Security Leader
Deloitte & Touche LLP
kheckel@deloitte.com

Sean Peasley
Partner
Global Enterprise Security Leader
Deloitte & Touche LLP
speasley@deloitte.com

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