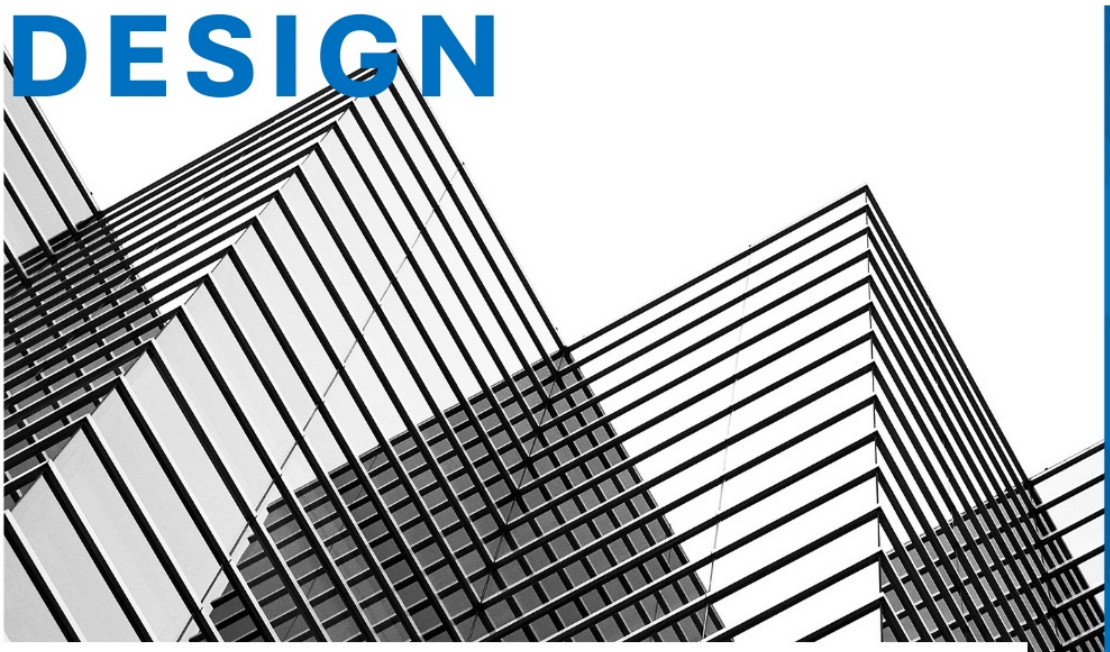
A GUIDE TO ADOPTING SECURITY BY DESIGN



ABOUT US

At Patterned Security, we provide modern approaches to enabling security by design.

There is an over-reliance in the industry on using generic ‘one size fits all’ security standards to determine what good looks like. Pushing endless lists of controls and distracting staff from focusing on what really matters.

Patterned Security is focused on supporting businesses in adopting practical solutions to cybersecurity.

EXECUTIVE SUMMARY

The Security by Design approach represents a foundational shift in how businesses conceptualise, plan, develop, and maintain security across their technology services.

At the heart of Security by Design is a holistic view that considers cybersecurity throughout project delivery and release management. From initial design to deployment and maintenance, security is a continuous concern that influences every decision.

Security by Design is predicated on the understanding that the cost of preventing security flaws is significantly less than the cost of fixing them post-release.

INTRODUCTION

The term "Security by Design" refers to the practice of incorporating cybersecurity into project delivery during its development and release stages rather than adding it later as an afterthought.

Security by Design has been widely used across various industries for several years.

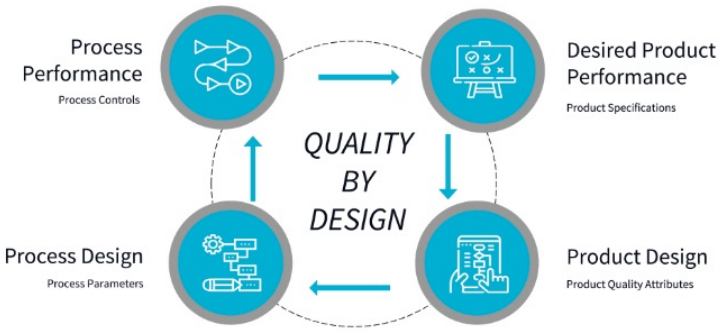
In more recent times, it has been used more extensively to reflect the increasing need for technology vendors and manufacturers to prioritise cybersecurity. "

UNDERSTANDING SECURITY BY DESIGN

The term 'security by design' is a concept derived from 'Quality by Design', a methodology widely adopted within the pharmaceutical industry.

We focus on drawing parallels between those two methodologies and on how security should be considered as important as quality in any project.

Quality by Design, akin to Plan-Do-Check-Act, is a customer-focused optimisation process that starts and ends with the customer. It emphasises enhancing features to increase customer satisfaction.



Security by Design (SbD) is not unique to the software manufacturing sector alone. We consider it applicable across all industries, with similar parallels in how cybersecurity is embedded in any project.

We define it as..

> ***"Security by Design is the process of embedding cybersecurity risk management across project delivery and release frameworks".***

We consider it applicable across all industries, with similar parallels in how cybersecurity is embedded in any project.

We draw parallels to the way they release platforms or systems into their environment, regardless of whether these are customer-facing.

For instance, consider a project establishing a new capability built on a cloud hosting platform. How does that project enable the consumption of the new service in a way that is 'Secure by Design' and 'Security by Default' for their internal teams?

WHY FOCUS ON SECURITY BY DESIGN

Many organisations begin their journey towards maturity by focusing solely on compliance with industry standards, such as ISO 27001 or SOC2 Type II. Many organisations are familiar with these industry standards and focus entirely towards just achieving certification.

While following these standards is beneficial, they typically describe a generic set of controls. Cybersecurity initiatives can then turn into mere 'checklist' exercises, which can detract from the main goal of enhancing an organisation's cyber resilience.

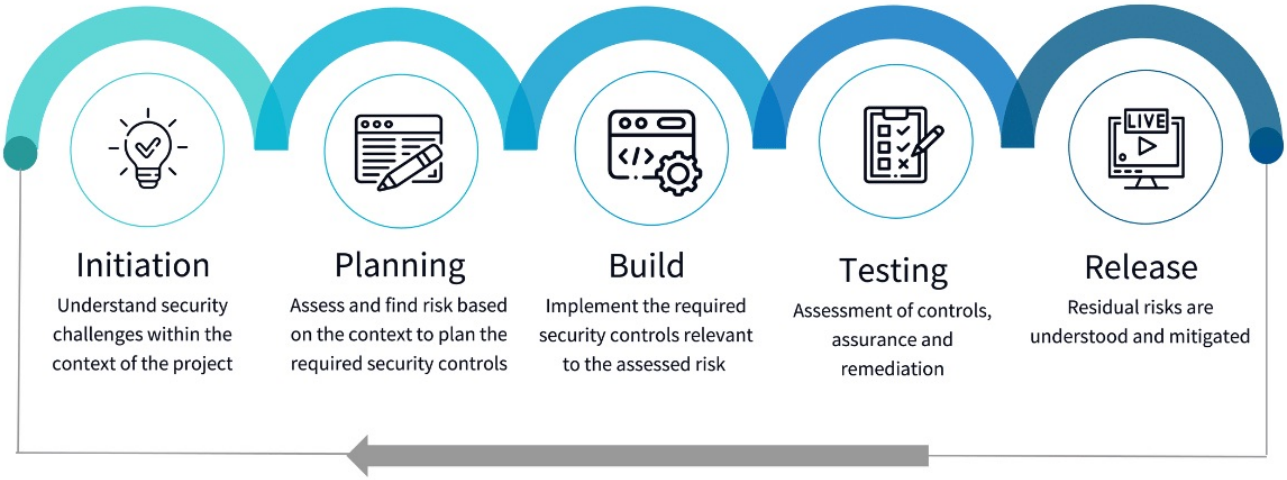
Security by Design begins with the fundamentals. The principles of Security by Design echo similar themes found in broader industry standards like ISO 27001 and SOC 2.

It can be difficult to get buy-in from your stakeholders when only talking on governance and risk management. Security by Design focuses on embedding cybersecurity into project release to provide more secure and higher quality outcomes.

GETTING STARTED WITH SECURITY BY DESIGN

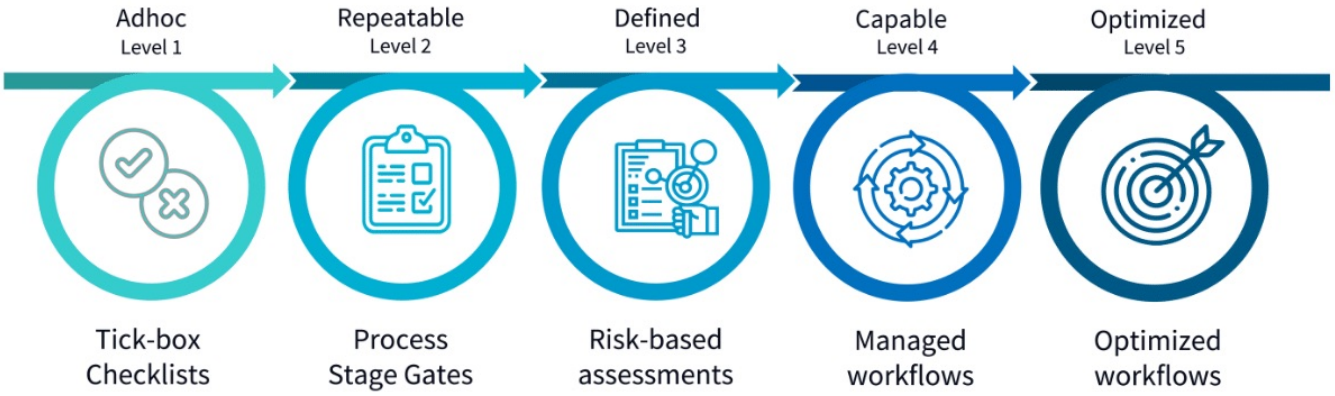
OVERVIEW TO SECURITY BY DESIGN

This is a summary view to how security is embedded into project delivery and release.



Every organisation has a different approach to project delivery. Whilst this may differ across different industries and sectors, the same journey towards maturity can be observed.

To help assist companies with the adoption of Security by Design, we've defined the following maturing levels providing a phased approach. We define the following five maturity levels.



This takes guidelines to both recent publications for Security by Design and based on Patterned Security own observations for the industry.

SECURITY BY DESIGN

LEVEL 1 | CHECK LISTS

At this initial level, your projects are just ‘ticking the box’ for a minimum set of controls that are easy to implement or derived from a security standard.

The challenge with this approach is that those ‘tick box’ controls often lack context regarding why these controls are necessary and what threats they address.

This lack of context can make it challenging for security architecture to evaluate risk when a requirement cannot be met. Security standards tend to make broad statements that are applicable to all use cases and often lose the context of the actual security threats and impacted assets.

LEVEL 2 | PROCESS STAGE GATES

In this phase, you've transitioned beyond basic checklists, establishing defined security checkpoints during the design, build, testing, and quality assurance stages.

There is executive endorsement for applying the principles of Security by Design and Security by Default. Cybersecurity has become incorporated into the design phase to understand requirements and identify necessary controls. This also includes understanding any specific security testing needed based on inherent risks.

You begin to form interactions with different teams or perspectives. Security teams will start to collaborate with solution architecture and design engineers to establish necessary security controls. However, maintaining consistency between the design phase and what is implemented and tested can be challenging. Process stage gates can be disconnected between architecture, testing and risk management functions.

To progress to the next level of maturity, companies need to consider how to involve risk management and stakeholder engagement in this process.

SECURITY BY DESIGN

LEVEL 3 | RISK-BASED ASSESSMENTS

At this level, you've adopted a risk-based approach to Security by Design. You'll be conducting initial assessments for inherent risks and threat modelling on the proposed solution.

The roles and responsibilities for Security by Design are more defined, enhancing workflows and interactions between different teams. The interaction process between the Architecture, Engineering, Testing and Risk Management teams is clearly outlined.

Checkpoints and stage gates are embedded within the project release phases and are measured accordingly.

Teams provide transparency to vulnerabilities and remediation, which may include

- Vulnerability disclosures, including a list of known vulnerabilities
- Publish Software Bills of Materials (SBOMs) for internally developed code or software

This is the point where many companies start to struggle with maturing their processes.

Architects and solution designers may continue to create varying types of design artefacts. Some are detailed or technical, while others are high level.

There's no consistency on how the different teams calculates and assesses risk.

LEVEL 4 | MANAGED WORKFLOWS

This is the point at which most organisations aim for maturity. There is traceability between inherent risk assessments, threat modelling, and selection of required controls.

Controls are selected based on the risks needed to protect technology assets and data.

Security patterns can address many of the key challenges discussed earlier regarding the use of just ‘checklist’ policies and standards.

SECURITY BY DESIGN

LEVEL 4 | MANAGED WORKFLOWS (CONTINUED...)

Risks are clearly understood based on threat modelling and inherent risk assessments for all project delivery.

A responsibility model is applied to individual controls, detailing which controls are configurable by consumers, and ensuring services are Secure by Default.

In this phase, we expect to have an executive sponsor for Security by Design to ensure adequate funding and resourcing.

Regular stakeholder reporting for maturity and conformance with Security by Design are provided based on defined metrics.

LEVEL 5 | OPTIMISED WORKFLOWS

This is the highest level of maturity, yet few organisations manage to achieve it. At this level, an organisation operates with a Security by Design council for governance and continuous workflow improvement.

Security Patterns are used consistently throughout project delivery to standardise and provide a structured model to connect various Security by Design phases.

These patterns also serve as a mechanism for a risk-based selection of controls. At this level, the organisation fully integrates security by design, fostering complete transparency and accountability.

Cybersecurity is strategically integrated within their methodologies, even incorporated into customer feedback and surveys. This approach effectively measures the performance of their security measures from the customers' perspective.

To maintain transparency and trust, the organisation may openly publish its Security by Design roadmap, sharing details about its successes and challenges encountered.

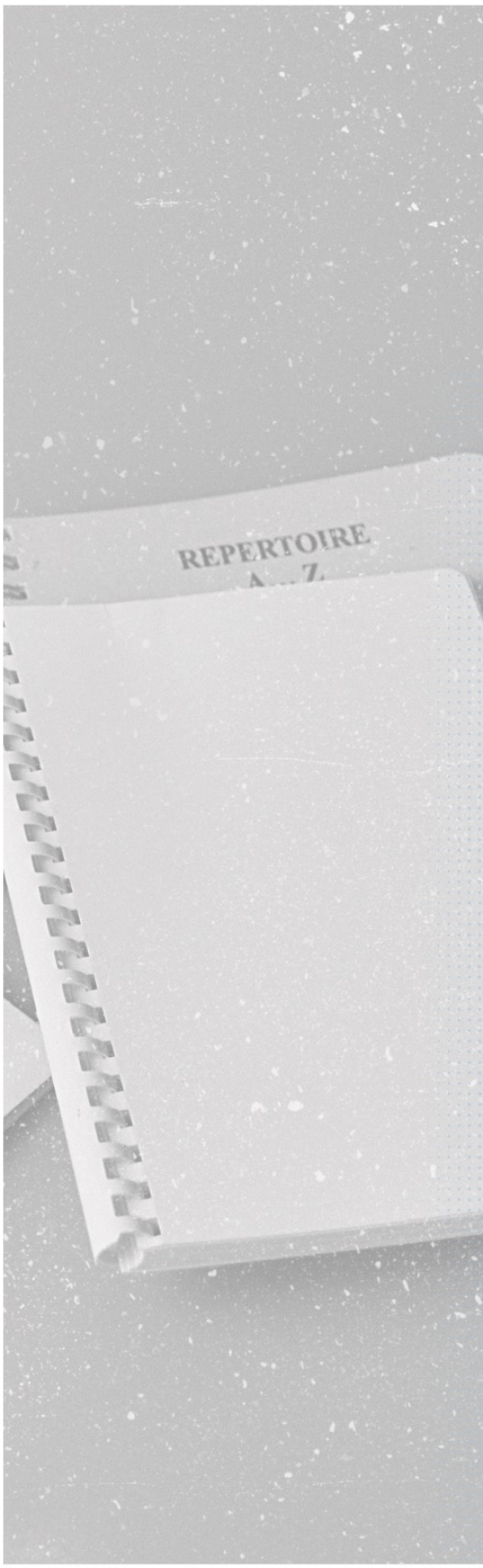
FINAL THOUGHTS

Security by Design is essential for creating secure, reliable, and trustworthy systems consistently. This approach prioritises security as a fundamental part of the development process, not an afterthought, offering a systematic framework for applying security patterns.

Incorporating security considerations from the onset enables the early detection and mitigation of potential cybersecurity flaws, promoting efficiency and cost-effectiveness. The Security by Design approach embodies the understanding that preventing cybersecurity flaws is less costly than fixing them after a product's release.

Moreover, this methodology fosters an organisation-wide consistency in implementing cybersecurity measures, thereby minimising the likelihood of cybersecurity defects or vulnerabilities. It advocates for a holistic perspective that views cybersecurity as a continuous concern throughout project delivery and release management.

As a result, Security by Design elevates the overall quality of the delivered projects by aligning it with the customer's needs and expectations for cybersecurity.



HOW CAN PATTERNED SECURITY HELP?

Our security by design accelerator program is specifically targeted at helping organisations improve their maturity.

This is a facilitated program that builds internal capability and staff training for enabling security by design in your company.

Our program is build around proven expertise and backed by our published methodology for Security Patterns.

Want to learn more?

Email us at
hello@patternedsecurity.com

SECURITY ARCHITECTURE CONSULTANCY
ISMS IMPLEMENTATION
SECURITY BY DESIGN ACCELERATOR PROGRAM