G-Cloud 15

SECURE BY DESIGN

Doc Ref No: ThalesGC1511

INTRODUCTION

Secure by Design (SbD) is an asset-based, risk-, and consequence- focused approach to the through-life management of cyber security and resilience.

The Thales UK Secure by Design (SbD) Service, is a risk based and consequence-informed approach to cyber security and engineering that embeds resilience, compliance, and assurance throughout the entire lifecycle. It transforms security from a bolt-on into a strategic enabler of mission success across Government Departments and regulated sectors such as Critical National Infrastructure (CNI) e.g. Aviation, Energy. Thales UK's Secure by Design service uses a proven in use delivery approach to couple an entire enterprise including safety, quality and supplier management to ensure end-to-end in policy, strategy, and operation. This approach has been used with multiple customers including major leaders in the automotive and aerospace sectors.

Thales UK provides templates, assurance frameworks, and lifecycle integration to ensure customers achieve demonstrable compliance with UK government-accepted security standards. The targeted standards include (but are not limited to) NCSC Secure by Design, CAF, Def-Stan 05-139, IEC62443, as well as current regulations like NIS, PTSI, the EU Cyber Resiliency Act and shall cover the UK Cyber Security and Resiliency Bill.

USE CASE

Secure by Design has become recommended and, in many cases, mandated to be applied to government, defence, CNI, health, and many other industry sectors. Application of the Thales UK Secure by Design Service gives an evidence-based, fact-driven case to assessors and auditors alike. Thales UK Secure by Design gives your governance structure confidence that Secure by Design is being integrated, controlled, and assured into your culture, supply chain, and delivery. Using the Thales UK Secure by Design approach will generate evidence to support your claim to meeting regulations, standards, and stakeholder expectations for secure delivery.

SERVICE DESCRIPTION

Features

- Integration of cyber security into every stage of the lifecycle from requirements capture through to deployment and out to disposal.
- Proactive not reactive, security is built in with a “left shift” and “right stretch” into the entire lifecycle.
- Aligns supplier assurance with UK MOD 05-139, NCSC Secure by Design and CAF.
- Consequence-informed, risk-based engineering, managing risk and end consequence by mission impact.
- Governance and taxonomies provisioning board-level visibility.
- Integration of security culture assessments, including human factors and insider risk into supplier assurance.
- Evidence-based readiness and assurance schemes.
- Multi-sector validity: Thales performs and has integrated Secure by Design across many sectors including defence, health, policing, and regulated industries such as Critical National Infrastructure (CNI).
- Strategic alignment across technical, operational, and cultural domains for holistic resilience.
- Asset-focused, consequence and risk based, threat analysis and threat modelling

Benefits

- Reduce your cyber risk exposure across OT and IT systems.
    - Secure by Design reduces cyber risk exposure by embedding security principles into the architecture, engineering, and operational lifecycle of both IT and cyber physical OT environments. Instead of bolting on controls post deployment, it ensures that Products, Systems, and Services (PSS) are inherently resilient, deterministic, and defensible from day one.

- Faster procurement cycles with pre-mapped assurance overlays.
    - Pre-mapped assurance overlays streamline procurement by front-loading the evidence, controls, and compliance artefacts that buyers typically need to validate late in the process. Instead of lengthy and costly repetitive cycles, suppliers and buyers work from a shared, pre-aligned assurance baseline.
- Improved stakeholder engagement through consequence-informed narratives.
    - Consequence-informed narratives strengthen stakeholders’ engagement by translating technical risk into operational, financial, and organisational impacts that decision-makers immediate recognise. Instead of abstract threat descriptions, stakeholders receive clear,

contextual stories that show why an issue matters and what it means for mission, service delivery and public trust.

- Demonstrable compliance with UK government security frameworks.
    - Secure by Design provides demonstrable, clear, and verifiable evidence that your organisation meets the security expectations set out in the UK government frameworks such as the NCSC Cyber Assessment Framework (CAF), and relevant sector-specific requirements. Instead of treating compliance as a paperwork exercise, it becomes a transparent, repeatable assurance mechanism that builds confidence across stakeholders, regulators, and supply chain partners.
- Left shift to find threats, consequences, and risks earlier.
    - “Left Shifting” means moving security thinking to the earlier possible stages of design and engineering, so threats, consequences, and risks are identified before they become expensive, embedded, or operationally dangerous. Rather than discovering design weaknesses during test, production or operation, Secure by Design brings threat modelling and resilience thinking into requirements, architecture, and early prototypes. This reduces rework, prevents insecure design patterns from taking root, and ensures that safety, resilience, and regulatory expectations are ingrained from the start.
- Protect customer, product and your reputation throughout product life.
    - Secure by Design protects customers, products, and reputations throughout the entire lifecycle by ensuring security and resilience are built in from the outset. By designing for safety and robustness the likelihood of vulnerabilities and undesired emergent behaviours are reduced, reducing potential for costly recalls or emergency patches. Evidentiary cases and arguments support regulator demands, produce traceability to threat models and support safety and security cases.
- Continuous assurance and risk management for better reaction to threats.
    - Continuous assurance means not relying on periodic audits or point-in-time tests, maintaining a live understanding of the security posture, allowing faster more, informed reactions to new threats and reducing the likelihood or operational disruptions.
- Maturity growth of product, service and solutions, meet government requirements.
    - The Thales Secure by Design solution accelerates the maturity of customers products, services, and solutions by embedding structured engineering practices, clear security baselines, and repeatable assurance processes. Customers are guided through a predictable, measurable improvement on security posture, resilience, and operational discipline. This uplift supports maturity growth in lien with regulatory expectations such as CAF, NIS, and PTSI, and Def Stan 05-139.
- Proactive risk management and link to SOC.
    - Proactive risk management identifies, prioritises, and mitigates threats before they reach production. Applying threat analysis provides clarity to required treatments, including controls and monitoring, allowing linkage to Security Operations.
- Continuous evidence-based approach to cyber security and DevSecOps.
    - Secure by Design underpinned by DevSecOps gains continuous evidence of compliance and resilience, reducing risk and accelerating delivery. Secure by Design defines the security and resilience principles to meet. DevSecOps is how to embed those principles into every build, deployment, and operational change, giving continuous assurance rather than point-in-tine testing.

DETAILED SERVICE OVERVIEW

The Thales UK Secure by Design Service Offering allows flexibility and adaptability to a customer's needs in moving them along their journey to value for cyber resiliency. Each mode of delivery will be based upon the level of maturity or change required by and agreed with a customer. Figure 1 shows the journey to value as an organisation progresses from cyber awareness to cyber resilience.

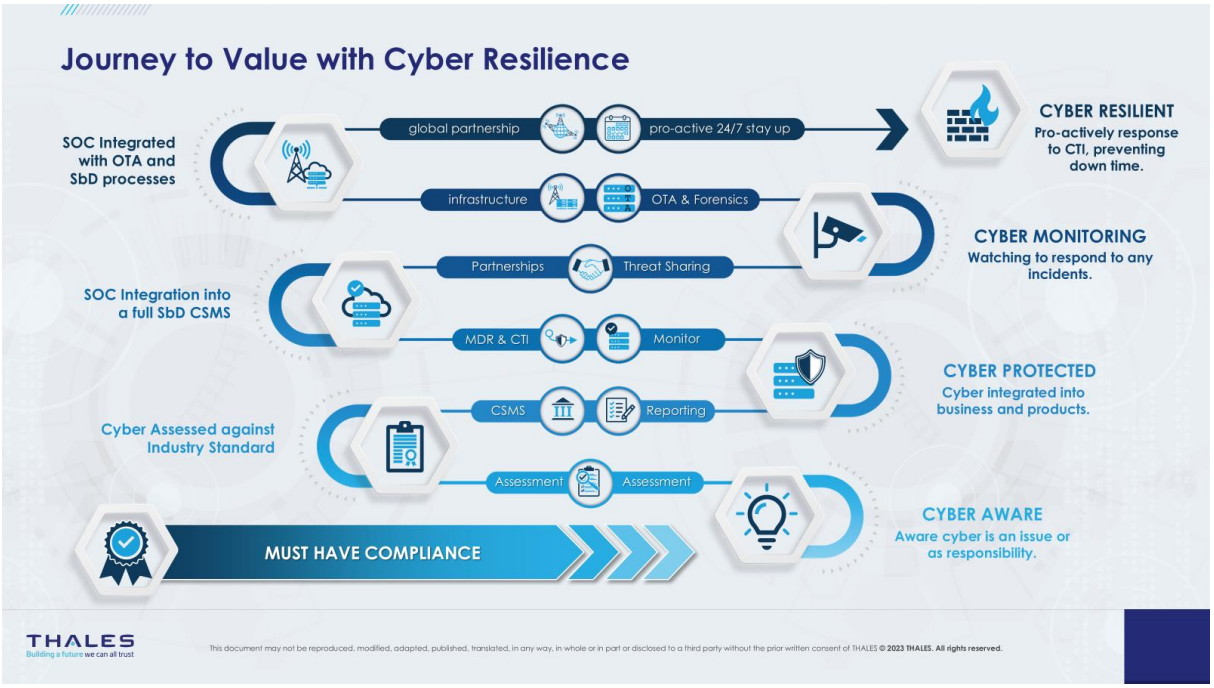


Figure 1 Thales UK Journey to Value with Cyber Resilience

Every Thales UK Secure by Design engagement is delivered by breaking it into 4 phases:

- Phase 1. Governance and Agreement
- Phase 2. Discovery: As-Is
- Phase 3. Planning to Deliver
- Phase 4. Execution

Each phase has specific objectives to be met, which are given below:

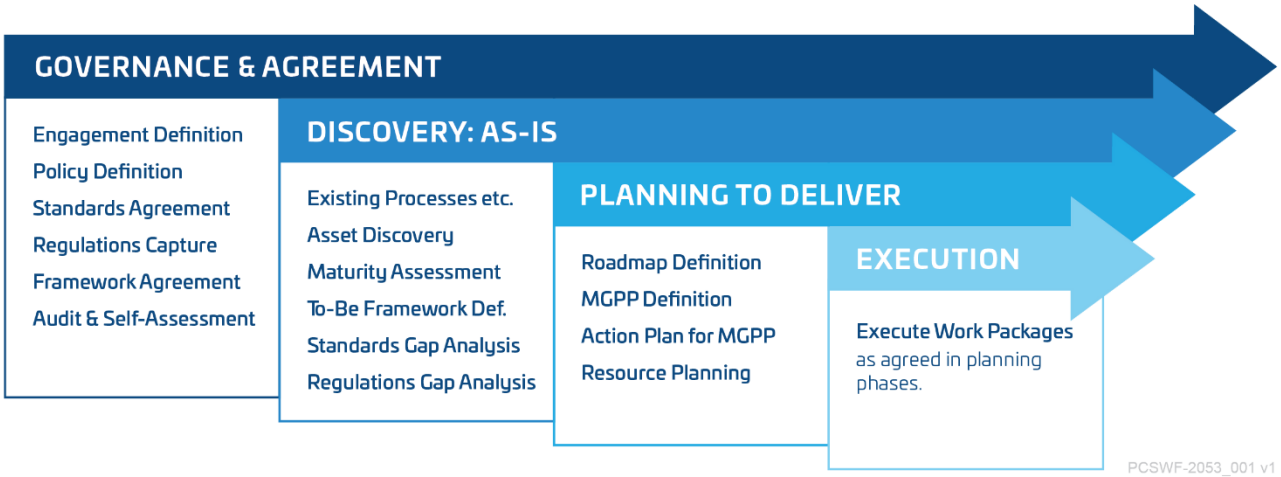


Figure 2 Thales UK 4 Phases of Secure by Design 4 Delivery

The Thales UK Secure by Design Service Offer can be applied in 4 modes of delivery:

- Mode 1. Cyber Security Management System (CSMS) Integration
- Mode 2. Secure by Design Integrator
- Mode 3. Secure by Design Advisory
- Mode 4. Secure by Design Consultancy

Mode 1, CSMS Integration, provides guidance and support to organisations integrating a new CSMS, or moving from one cyber security framework, system, or operational model to another.

As an example, a customer already has a team performing cyber security development for their products but wants better integration of their processes and governance into their enterprise structure and culture. At the other end of the spectrum, a customer new to the need for product cyber security needs help to integrate product cyber security into their enterprise operating model. Thales helps customers define the structure of their Product Cyber Security Management System and develop the appropriate templates and documentation to support its execution.

Mode 1 is an enterprise transformational mode, performing the integration of a Cyber Security Management System to tightly couple the execution of product design with cyber security, and integrate them into an existing enterprise operational model.
Thales has extensive experience in applying this mode into manufacturing, automotive, and aerospace industries.

Mode 2, Secure by Design Integrator, focuses on the customer's journey to value for Secure by Design, ensuring cost effective integration of tools and services into an enterprise already on the journey to integration of Secure by Design. An example use case for this mode may be a customer that has already had some discussion on how to effectively pursue Secure by Design but is looking for support in identifying and planning their next steps in the actual execution. This may involve developing an understanding of what cyber security tooling and features their enterprise needs for developing their products and how to integrate tools and processes into their existing processes to achieve a Secure by Design Cyber Security Engineering Process (CEP).

Modes 1 and 2 are focused on business process definition (CSMS) and engineering process (CEP) execution respectively. However, if a customer is looking to have a supplier perform full business process integration with potential for tool integration support, modes 3 and 4 are offered as holistic end-to-end services.

Modes 3 and 4 take a customer through the entirety of Secure by Design and Cyber Resilience integration and transformation. The difference between Mode 3 and Mode 4: Mode 3 focuses on giving advice, Mode 4 focuses on consulting and executing upon the consultancy results.

For example, a customer may already be aware of their needs and may be looking for support in moving forward with their maturity. Here **mode 3, Secure by Design Advisory** can be appropriate to help shape client strategic direction, governance, policy alignment, and security culture. Mode 3 is a more hands-off approach where Thales UK supports the strategic intent for a customer making progression to a fully cyber resilient enterprise. Typically, Mode 3 will take a customer up to and including Phase 3 – Planning to Deliver, stopping short of operational delivery.

Alternatively, a customer may need support in understanding where they are on the Secure by Design Journey to Value, requiring detailed assessment, guidance and possibly even hands-on implementation in their action planning and execution. In this case **mode 4, Secure by Design Consultancy** would be of most benefit. Thales UK Secure by Design Consultancy provides operational enablement, hands-on implementation, technical design, guidance, and troubleshooting for the holistic integration of Secure by Design.

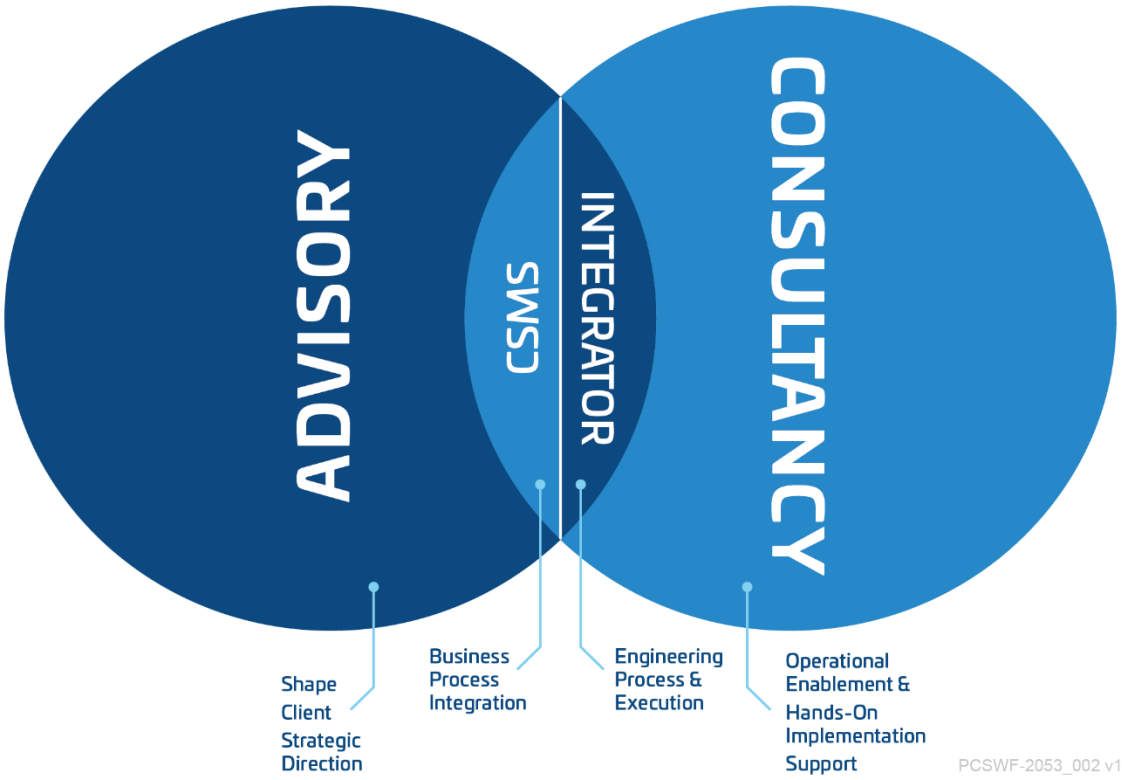
To help a customer decide where they need help from Thales UK, the table below shows Modes 3 and 4 against each other:

	Advisory	Consultancy
Purpose / Scope	Shape client strategic direction, governance, policy alignment, and security culture	Operational enablement, Hands-on implementation, technical design, guidance, and troubleshooting
Engagement Model	Periodic, high-level consultations with leadership or architecture boards	Ongoing project-embedded, working closely with engineering to provide responsive assistance to delivery teams and stakeholders
Typical Output	Security roadmaps, maturity assessments, policy frameworks, risk posture reviews	Implementation guidance, artefact reviews, Q&A sessions, tooling support, architecture design guidance, threat modelling guidance, implementation guidance, and assurance plan guidance
Client Maturity Fit	Ideal for organisations shaping or refining their SbD strategy	Best for teams actively operationalising or applying SbD principles in live projects
Target audience	CISOs, Architects, programme leads	Product teams, engineers, delivery managers
Value Proposition	Align security with business objectives and regulatory frameworks	Reduces delivery friction and improves assurance outcomes in real time
Example Deliverables	Workshops, board briefings, strategic reports, SbD operating model, threat landscape analysis, policy alignment	Tools, templates, processes, work instructions, execution guides, and training material

Thales UK Secure by Design is an asset-focused, risk and consequence based, through-entire-life approach to cyber resiliency. Modular in construction, Thales UK Secure by Design can draw upon a vast array of expertise, tools, solutions and associated products to give customers a resilient future they can depend upon. An engagement with Thales UK is a customer delivery focused. With Thales UK the customer is priority, and the common starting point is the customer context. The customer can start with any mode and switch as required, drawing in Thales UK broad spectrum of resource competences.

Thales UK Secure by Design pedigree is credibly evidenced as:

- **Standards-shaping**: Authors and implementers of the MoD DefStan for Secure by Design.
- **Lifecycle-driven**: A proven SbD integration approach that left shifts resilience and embeds it though the entire lifecycle.
- **Assurance-ready**: Traceable to UK standards and backed by NCSC accredited cyber consultancy.
- **CNI-proven**: Actively securing UK government, law enforcement, and critical national infrastructure, including OT environments.



Examples of how Thales UK Secure by Design can draw upon wider solutions to construct the specific needs of individual customers includes:

- Experience across many industries in applying many standards and practices.
- Draw upon experience and expertise in security verification & validation.
- Practical application and experience of security operations and monitoring services.
- Threat analysis to define and monitor residual risk to an enterprise or product (STRAT).
- Practical integration and application of PKI, HSM and security infrastructure solutions.
- Assessing true Root Cause Analysis into a customer's security needs.
- Utilisation of Plan, Do, Check, Act into the integration of Secure by Design.
- Deep seated knowledge of human factors upon Secure by Design.

ABOUT THALES

Thales in the UK has been harnessing technology to benefit the nation for over a century. Across all walks of life, you will find us securing and protecting every moment. We develop world-leading capabilities to help our customers think smarter and act faster.

Thales collaborate with partners in both government and industry, providing cutting-edge technologies to the civil and defence markets.

Thales has a significant presence across the UK, with locations strategically positioned in England, Wales, Northern Ireland, and Scotland. This geographic reach enables us to effectively support the diverse needs of local communities while contributing to the economic prosperity of all four nations. Our key facilities, along with several customer-facing sites, extend from the South West of England to Glasgow, reinforcing our commitment to regional investment and development.

The most trusted organisations in the world rely on Thales for cybersecurity solutions that keep critical assets safe. With more than 6,000 cybersecurity experts worldwide, our portfolio protects applications, data and identities, including services that close compliance gaps, detect and monitor threats and strengthen defences.

For further information, please see https://www.thalesgroup.com/en/worldwide/united-kingdom