Cyberfort

WHITE PAPER

Understanding Secure by Design – Unlock the benefits of adopting this proactive approach to cyber resilience

Secure by Design

The National Cyber Security Centre (NCSC) have been advocating the adoption of Secure by Design (SbD), when they published their own Principles in 2019. Since then, the Ministry of Defence, Government Digital Services and the UK Government Security Function have all published and adopted their own versions of the Principles and associated activities that should be expected by Government departments and supply chains to adopt SbD as an approach to managing risks to the delivery and use of digital services.

Emerging cyber threats can appear at pace and scale; therefore, it is essential that organisations understand and prepare to address and respond to cyber threats that may impact their business. Secure by Design Principles lay the foundations for organisations to do just that.

Cyberfort blends cyber security skills and experience of Security Architecture, Governance, Risk, and Compliance (GRC), Security Operations and Testing to help organisations implement these Secure by Design principles effectively — balancing security, functionality, risk appetite, and regulatory obligations with Business needs. Together, these specialists provide the expertise, oversight, and governance required to embed security into business operations and technology estates.

This white paper explores the SbD principles and activities, outlines challenges faced by organisations, and highlights the benefits of adopting this proactive approach to cyber resilience.

Introduction

As digital services become central to delivering government functions and interacting with the public, the threat landscape has evolved. High-profile breaches, ransomware attacks, and data leaks have demonstrated the significant consequences of security weaknesses. In response, the UK Government's Secure by Design (SbD) principles provide a robust framework to ensure that digital services are secure from the outset and remain resilient throughout their lifecycle. These ten principles align with best practices from the NCSC, drawing on decades of cyber defence expertise, forming the foundation of a resilient, proactive security posture that prioritises responsibility, secure technology sourcing, risk-based approaches, and flexible architecture. They aim to move organisations beyond reactive security models, embedding security responsibilities and controls early and throughout system design, development, and operation.

Overview of the 10 Secure by Design Principles
The ten principles advocated by the UK Government Security function address key aspects of building, operating, and evolving secure digital services, they are mandatory for government departments and arm's length bodies (ALBs), and optional for other parts of the public sector.

01 Create Responsibility for Cyber Security Risk

02 Source Secure Technology Products

03 Adopt a Risk-Driven Approach

04 Design Usable Security Controls

05 Build in Detect and Respond Security

06 Design Flexible Architectures

07 Minimise the Attack Surface

08 Defend in Depth

09 Embed Continuous Assurance

10 Make Changes Securely

01 Create Responsibility for Cyber Security Risk

By considering security within the business case for digital services, agreeing the roles and responsibilities necessary to identify the relevant security resources, the activities of this Principle aim to ensure that Cyber Security is considered at the senior leadership level within the context of the organisation and project risk appetite. Successful implementation of this Principle will ensure that appropriate resources are made available to manage security risks throughout the lifecycle of the service.

02 Source Secure Technology Products

Managing third party risks and adopting measures to identify security weaknesses, the activities of this Principle aim to assess the security attributes of technology before adoption. Where suppliers provide products this Principle aims to implement measures to understand the risks associated with the software and hardware supply chain.

03 Adopt a Risk-Driven Approach

Establishing the project's risk appetite and maintaining the assessment of cyber security risks helps build protections appropriate to the evolving threat landscape. This supports the intended outcome of this Principles "A Dynamic risk management process that can respond to emerging threats" (More information on this can be found on the UK Government's Secure by Design website). However, the organisation must successfully embed a range of activities in order to effectively achieve this outcome including: inventorying assets, performing threat modelling, agreeing a baseline of security controls, having response measures and the appropriate resource to respond to risk conclusions and managing service assets and components through-life, disposing of them securely when retired.

04 Design Usable Security Controls

Many of the activities already mentioned in the first 3 Principles support this princple the outcomes of which should be a service with security designed that supports user journeys and avoids poor security practices by removing the temptations of workarounds. Additional activities that support the maintenance of this Principle ensure that regular user research and the testing of control efficacy contribute to service and security assessment of weaknesses that can be addressed.

05 Build in Detect and Respond Security

Security vulnerabilities are inevitable and the integration of appropriate security logging, monitoring, alerting and response capabilities is essential to identifying weaknesses, these must be continually tested and iterated. An effective capability to detect, respond to and recover from incidents leads to lower business impact, Principle 5 relies on controls testing, vulnerability management which in turn leads to fewer weakness.

06 Design Flexible Architectures

Technology evolves rapidly, and threat actors adapt their methods. By responding to and mitigating security risks and assessing the effectiveness of security controls, by undertaking key activities of this Principle organisations can ensure that changes can be made without compromising on security, supporting faster response to evolving cyber threats. By designing with change in mind, modular, scalable, without undermining existing controls, services can be future-proofed through resilience and adaptability.

07 Minimise the Attack Surface

Use of only the components necessary to mitigate cyber security risks while achieving its intended use. Successful adoption of previous Principles, organisations already establish a baseline of activities necessary to reduce the number of exposed components, services, and access points which decreases the likelihood of exploitation. Asset management, risk management, vulnerability management, threat modelling and identification continue to support reducing opportunities for attack and increase the cost effectiveness of operating and maintaining the service.

08 Defend in Depth

Defence in Depth is not a new concept but is one that SbD reinforces the need for. Layered security ensures that if one defence is bypassed, additional controls remain in place reducing the likelihood of compromise. The application of specific controls such as endpoint protection, access controls, network segregation, encryption, and continuous validation increases the time, effort and cost to an attacker and keeps the impact of vulnerabilities more contained.

09 Embed Continuous Assurance

Security assurance continued throughout a system's lifecycle provides risk owners with evidence that controls and capabilities are operating as intended. Regular audits, testing, configuration validation, and policy enforcement are necessary to confirm that systems remain secure after deployment verifying that the service continues to mitigate the identified risks. The activities to support this are already built into the security programme if SbD has been adopted effectively, tracking the organisations progress through the adoption of SbD support this Principle and ensures that gaps in the approach can be resolved.

10 Make Changes Securely

All changes should be governed by secure change management processes. This ensures the introduction of unintended consequences can be avoided and maintains audit trails for accountability. Security impact assessments and rollback plans are critical components. Managing the security risks of the service within your risk appetite from the start of your project and throughout the service life cycle reduces the risk of introducing weaknesses into the service that could cause potential data breaches, disruption, or open up routes for attackers into your whole organisation.

Implementing Secure by Design

Cyberfort ensures cyber security and resilience is built into systems, processes and policies from the start of a product or service lifecycle. This enables organisations to align security with business objectives, existing systems, and industry regulations. This Secure by Design approach empowers organisations to understand and improve security throughout a product or service lifecycle. Implementing these principles requires cross-functional collaboration, cultural change, and investment in people, processes, and tools. In the next section of this white paper we explore the approaches for performing Secure by Design practices.

Approaches to Embedding Security into Organisational Culture
A security-first mindset must be embedded across departments to ensure cyber risks are effectively managed. Central to this is **Principle 1:** Create responsibility for cyber security risk, which emphasises that accountability must be clearly defined. Senior leaders, service owners, and delivery teams all have roles to play in identifying and mitigating risks across the lifecycle of government services.

A mature security culture supports transparency, encourages responsible reporting, and values continuous learning. Staff must be empowered through role-specific training, and policies should reinforce expectations without hindering delivery. By fostering a culture where cyber security is understood as a shared responsibility, organisations can embed secure practices as the norm rather than an exception.

Integrating Security in the Development Lifecycle
Secure by Design is most effective when applied from the outset of service development. **Principle 3:** Adopt a risk-driven approach ensures that services are designed based on a clear understanding of context, threats, and potential impacts. **Principle 4:** Design usable security controls supports the development of solutions that are both effective and accessible, reducing the likelihood of users bypassing controls out of frustration.

Security must be integrated into each phase of the delivery lifecycle—discovery, design, build, test, deploy, and decommissioning. This includes using secure-by-default configurations, dependency management, and regular risk assessments. Following **Principle 10:** Make changes securely, all changes should go through secure, auditable processes, with appropriate testing and rollback procedures.

Leveraging Technology and Automation
Modern government services operate at scale and pace, making automation essential for consistent and timely security outcomes. By applying **Principle 5:** Build in detect and respond security, services can benefit from proactive monitoring and incident detection systems, enabling early intervention and mitigation.

Adopting **Principle 9**: Embed continuous assurance means using automation not only for threat detection, but also for compliance, testing, and reporting. Continuous integration pipelines can integrate code scanning and policy enforcement, ensuring security doesn't become a bottleneck. These automated measures support rapid delivery without compromising resilience.

In tandem, **Principle 6:** Design flexible architectures allows services to evolve safely, adapting to emerging technologies and new threats without fundamental redesign should also be implemented at this stage.

Collaborating with Internal and External Stakeholders
A blend of Cyber security skills and experience across disciplines such as Security Architecture, Governance, Risk, and Compliance (GRC), Security Operations and Testing effectively help organisations implement these Secure by Design principles. This collaborative approach to security assurance ensures that relevant subject matter experts input to the design or change, risk identification and management is effective and timely.

Government services rarely operate in isolation; they rely on technology vendors, partners, and shared infrastructure. **Principle 2:** Source secure technology products requires departments to assess and select suppliers that meet rigorous security standards. Supply chain assurance must be ongoing, not a one-time checkpoint.

Challenges in Implementing Secure by Design

Despite its value, implementing Secure by Design can encounter obstacles. These include legacy systems, skill shortages, bureaucratic inaction, and competing priorities. Cyberfort's approach, evolved from working with multiple Government departments removes focus on just achieving compliance and the pressures on the delivery and design teams. It empowers teams across an organisation to identify and manage security risks early in the lifecycle and offers the opportunity for innovation throughout a product or service lifecycle

Legacy Systems and Technical Debt

Many government departments continue to rely on ageing infrastructure and legacy systems that were not designed with modern security principles in mind. This poses a direct challenge to Principles 6: Design flexible architectures and 7: Minimise the attack surface. Retrofitting security into outdated systems is often costly, complex, and may offer only partial coverage. Technical debt also limits agility, making it harder to respond to emerging threats or implement contemporary detection and response capabilities (Principle 5). A clear risk-driven roadmap is needed to gradually modernise systems, guided by Principle 3: Adopt a risk-driven approach, while maintaining continuity of essential services.

Skills and Resource Gaps

The Department for Science, Innovation & Technology have highlighted the cyber skills shortage in the UK labour market over several years. Recruiting, training, and retaining qualified professionals are crucial to delivering Secure by Design. Investment in apprenticeships and knowledge transfer is essential. Delivering secure-by-design outcomes requires a multidisciplinary workforce with expertise in cyber security, secure architecture, DevSecOps, procurement, and policy. However, attracting and retaining these skills remains a challenge, particularly in a competitive labour market. This impacts the organisation's ability to fully implement Principle 1: Create responsibility for cyber security risk, as responsibilities may fall to individuals or teams without the depth of knowledge required.

Additionally, the lack of security awareness among non-specialist staff can hinder effective implementation of Principle 4: Design usable security controls. Bridging the skills gap requires not only specialist recruitment but also the upskilling of existing staff and fostering collaboration across disciplines.

Competing Priorities

Government organisations often face intense pressure to deliver digital services rapidly, especially under political or operational deadlines. This can result in security being deprioritised in favour of speed or functionality. Such trade-offs directly undermine Principle 9: Embed continuous assurance and Principle 10: Make changes securely.

Security must be embedded as a non-negotiable requirement rather than treated as a compliance checkbox. Balancing delivery pressures with long-term security needs requires strong leadership, realistic timelines, and a clear understanding of risk—reflecting Principle 3 once again. Without this, security may be seen as a blocker rather than an enabler of sustainable, trusted services.

Supply Chain Complexity

Government services increasingly depend on external vendors, cloud platforms, and off-the-shelf solutions. Ensuring that these suppliers meet Secure by Design standards is challenging but critical, particularly under Principle 2: Source secure technology products. Supply chain vulnerabilities can become systemic risks if not properly assessed and managed.

Compounding this is the difficulty of maintaining visibility across supplier practices, dependencies, and sub-processors. Implementing Principles 7 and 8: minimising the attack surface and applying defence-in-depth requires not just contractual controls but ongoing supplier assurance, penetration testing, and coordinated incident response planning.

Change Management and Bureaucracy

Implementing Secure by Design often requires significant organisational change, revised governance, new technical controls, process updates, and cultural shifts. Yet public sector organisations can be risk-averse, process-heavy, and slow to adapt. This poses barriers to Principle 10: Make changes securely and undermines Principle 5, which calls for regular evaluation and improvement.

Clear accountability structures (Principle 1) and streamlined change control processes are necessary to overcome inertia. Embedding security into existing governance structures, rather than treating it as an add-on, helps align it with core delivery goals and reduce resistance.

Benefits of Implementing Secure by Design

The rewards of Secure by Design extend beyond compliance. It fosters confidence in services, minimises risk, and supports digital transformation. By working with Cyberfort as your Secure by Design partner, you will improve risk identification and management throughout a product or service lifecycle, manage regulatory risks as products and services evolve and align security with your business objectives.

Enhanced Service Resilience

By integrating security from the outset, government services become inherently more resilient to cyber threats and operational disruptions. Applying Principle 5: Build in detect and respond security ensures that systems are protected against attacks but also capable of identifying and recovering from them quickly. Combined with Principle 6: Design flexible architectures, this allows services to adapt to changing threats, manage incidents in real time, and continue delivering critical functions under pressure.

Resilience is further strengthened by Principle 8: Defend in depth, which advocates for layered defence across infrastructure, applications, and endpoints. A single point of failure is less likely to result in service compromise, making systems more robust and reliable in the face of attacks.

Compliance and Audit Readiness

Adopting Secure by Design practices makes it significantly easier to meet statutory, regulatory, and assurance requirements. Principle 9: Embed continuous assurance supports a proactive approach to governance by enabling real-time visibility into system health, configuration drift, and control effectiveness.

Security controls, when built into service design, allow for faster, more confident responses to audits and assurance reviews. Documented roles and responsibilities under Principle 1: Create responsibility for cyber security risk and provide clear lines of accountability, while adherence to Principle 3: Adopt a risk-driven approach ensures that compliance measures are proportionate and justifiable. This readiness not only satisfies oversight bodies but also instils internal discipline and improves operational efficiency.

Reduced Cost of Incidents

The long-term financial benefits of Secure by Design are substantial. Principle 7: Minimise the attack surface helps reduce exposure to vulnerabilities, while Principle 2: Source secure technology products lowers the risk of introducing insecure components into critical systems.

By preventing breaches before they occur and responding more quickly when they do, organisations can avoid the high costs of downtime, data loss, legal liability, and reputational harm. Investing in security early in the development lifecycle also reduces the need for costly rework, reflecting the principle of making changes securely (Principle 10). Prevention, detection, and recovery mechanisms combine to significantly lower the total cost of ownership across digital services.

Improved Public Confidence
Public services handle some of the most sensitive personal and financial data in the UK. Demonstrating strong cyber security practices directly supports Principle 4: Design usable security controls, ensuring that users feel confident engaging with services without compromising their privacy or safety.

Furthermore, visible commitment to security through transparent incident handling, clear communication, and continuous improvement—builds trust over time. A SbD approach sends a strong message that government services are designed with citizens' interests in mind, reinforcing confidence in digital transformation and the responsible use of data.

Innovation Enablement
Far from being a constraint, Secure by Design can actually accelerate innovation. By embedding scalable and adaptable architectures (Principle 6) and clear governance structures (Principle 1), organisations create an environment where new ideas can be tested safely and deployed confidently.

Security becomes an enabler when it integrates into delivery pipelines and is not bolted on afterwards. Developers and architects can build and iterate faster, knowing that automated controls and risk-based guidance are in place. This empowers departments to adopt emerging technologies and evolve services whilst understanding and managing the risk of doing so.

Final Thoughts

Cyberfort Secure by Design services enable organisations to implement the foundations required for embedding cyber security practices in information systems and digital delivery, building resilient digital services.

The Secure by Design principles offer a robust, practical framework for embedding cyber security at the heart of service delivery. In an environment where digital transformation is accelerating and threats are increasingly sophisticated, these principles and supporting activities provide the necessary foundation for building resilient, trusted, and accountable public services.

Secure by Design is not a standalone initiative or a tick-box exercise. It is a comprehensive approach that requires security to be integrated across governance, culture, development, technology, and partnerships. It begins with creating clear responsibility for cyber security risk (Principle 1) - ensuring that roles and accountabilities are unambiguous, and that senior leaders are actively involved in managing and owning cyber risk.

By sourcing secure technology products (Principle 2) and adopting a risk-driven approach (Principle 3), departments can make informed, context-specific decisions that align security investments with business needs and threat profiles. This approach ensures resources are applied proportionately, avoiding both over-engineering and unnecessary exposure.

Designing usable security controls (Principle 4) further reinforces the importance of balancing protection with accessibility. Services must allow staff and citizens alike to interact securely without undue complexity. This principle strengthens not only the technical robustness of systems but also their usability, compliance, and adoption.

Through embedding detection and response capabilities (Principle 5) and designing flexible architectures (Principle 6), organisations can monitor, adapt, and recover; key attributes in a world where cyber threats evolve daily. These principles support operational continuity and reduce the impact of incidents, enabling services to remain reliable and responsive under pressure.

The technical foundations of Secure by Design - minimising the attack surface (Principle 7) and defence in depth (Principle 8) - ensure layered, resilient protection. Together, they reduce the chances of compromise and ensure that if one control fails, others continue to protect core assets. This layered approach is particularly critical in complex environments where services depend on a multitude of components, both internal and external.

Continuous assurance (Principle 9) ensures that security remains effective. Security controls should evolve as threats, technology, and business models change. This principle promotes a culture of continuous improvement and accountability, aligning with agile delivery models and modern DevSecOps practices.

Finally, making changes securely (Principle 10) ensures that updates, patches, and new features are introduced without creating new vulnerabilities. As digital services evolve, change becomes a constant - making secure change management essential to maintaining trust, performance, and compliance.

Cyberfort works with organisations to make sure cyber security and resilience is built into systems from the beginning, embedding the principles through collaborative working with client delivery teams, so that security is aligned to the organisations objectives and integrated with systems as design evolves.

Discover more about Cyberfort's all-encompassing Cyber Security Services

At Cyberfort we provide a range of customers with all-encompassing Cyber Security Services. We are passionate about the cyber security services we deliver for our customers which keeps their people, data, systems and technology infrastructure secure, resilient and compliant.

Our business offers National Cyber Security Centre assured Consultancy services, Identification and Protection against cyber-attacks, proactive Detection and Response to security incidents through our security operations centre and a Secure and Recover set of Cloud solutions which keeps data safely stored, managed and available 24/7/365.

Over the past 20 years we have combined our market leading accreditations, peerless cyber security expertise, strong technology partnerships, investment in our future cyber professionals and secure locations to deliver a cyber security experience for customers which enables them to achieve their business and technology goals in an ever-changing digital world.

For more information on our Consultancy services please contact us at the details below:

+44 (0)1304 814800 | info@cyberfortgroup.com | https://cyberfortgroup.com

We look forward to working with you