# MoD Secure by Design (SbD)

WHITE PAPER

Aug 2023

# TABLE OF CONTENTS

## Introduction

There are very few threats that are faced by individuals, organisations and governments alike; at the precipice of them all, in our current age, are cyber-attacks. Any number of actors, be they state-backed, hacktivists or organised criminals, have the potential to circumvent the security procedures and barriers created to protect information of value.

The UK Ministry of Defence (MoD) has now released a new policy for managing the through-life cyber security of projects and programs, to prevent unauthorised access to sensitive information, and supply a robust, future-proof method to protect IT services and to serve in defence of the UK and its allies.

## What is 'Secure by Design'?

Secure by Design (SbD) is a process where security is incorporated into the scoping and development of IT projects and programs as an 'essential aspect'. It ensures data and information is protected from the outset and at every stage of development and delivery. It is not an added extra that is included retrospectively in a project's lifecycle (pre- or post-launch).

SbD is inherently similar to the Software Development Lifecycle (SDLC) - now a widespread industry practice – which usually contains the following phases:

- Requirements
- Analysis
- Design
- Development
- Testing & Verification
- Deployment
- Maintenance & Evolution

Examples of SDLC include the 'Waterfall' model developed in the 1970s, or the 'Agile SDLC' model, first published in 2001. SbD is an integrated approach to security development and architecture, developed by the MoD for their internal projects.

## How does this approach differ from before?

The MoD states: '*The Secure by Design approach is a modern approach whereby SROs, capability owners and delivery teams are accountable and responsible for delivering systems that are cyber secure. Safety isn't treated as an add on or an optional extra that can be traded out and cyber security needs to be treated the same*' (Secure by Design – a new way to manage cyber risk in capabilities - Defence Digital (blog.gov.uk)).

Many IT projects, until recently, would be scoped and initiated looking to complete a requirement and achieve the aim - within budget and on-time - with cyber security being added retrospectively to address an unforeseen security omission, or to adhere to a security framework (i.e., 'Accreditation').

The cyber security industry is now beginning to address the issue of insecure applications and programs, by having security built in from the inception of developing projects - ensuring security is no longer seen as a blocker or 'bolt on'.

The MoD SbD process will be a move from the previous accreditation service to a second line assurance function - which will perform independent assessments of MoD capabilities on a case-by-case basis. This means projects will need to continuously prove they are maintaining cyber security to current standards, instead of attaining a 'one-off' certification. This will make MoD IT systems inherently more robust to attack, ensure they are monitored more regularly and capable of defending against current and emerging cyber threats.

## How will the MoD do this?

A pilot scheme has been running since 2022, with 40 programmes finding new ways of working to date, allowing the Secure by Design team to create policy, processes and guidance and tooling throughout the process. All new MoD programmes must adopt the SbD approach.

The 5 steps for MoD SbD:

1. Prepare
2. Control Frameworks, Designing for Security, Maturity Assessments
3. Testing
4. In-Service
5. Disposal/Termination

## Stage 1: Prepare

A self-assessment tool (taken from NIST SP 800-37 Rev 2) will enable projects to manage their maturity against security policy (i.e., JSP440 Leaflet 5C 'Building Cyber Secure by Design Capabilities', JSP604, etc.) and technical guidance, tracking progress and identifying areas that need to be incorporated.

Cyber security is now being listed as a 'key capability requirement' – meaning projects need to incorporate, resource and fund it, like any other requirement.

## Stage 2: Control Frameworks, Designing for Security, Maturity Assessments

SbD will use the NIST (National Institute of Standards and Technology) 800-53 Rev 5 Cyber Security Framework (CSF) controls for projects near entering service. Projects already in service will be assessed against this framework, as they migrate from the traditional accreditation process to continual assurance under the SbD process.
However, if another CSF is more appropriate, or controls need to be adjusted/amended, others can be used. Appropriate risk management frameworks should always be used (such as NIST 800-37 Rev 2).

There will also be two main types of assurance used in SbD: 'Programme' (self-assessment) and 'Independent' (external assurance for high-risk programmes).

## Stage 3: Testing

Projects will be required to conduct continual security testing and risk assessments. These will include testing of concepts and architecture, as well as functional security and NCSC Assured CHECK scheme penetration testing.

## Stage 4: In-Service

All systems, services and products will need to maintain their cyber security posture, throughout the time in-service as part of in-service planning. This includes the resources, systems and techniques used.

## Stage 5: Disposal/Termination

Continuous assessment will help managers determine if a project has reached its productive limit or the end of its planned lifecycle. When this happens, decisions need to be made about how to handle the data and services used, including their security classification.

The security classification will then dictate the appropriate manner of disposal to be used.

## How can AMR CyberSecurity help?

AMR CyberSecurity is a CREST Certified, NCSC CHECK penetration testing service provider. Our consultants have years of first-hand experience working within the UK MoD Security apparatus. We can provide assurance insights into projects and programs at any level of the design and implementation process, to ensure that MoD Secure by Design principles are being adhered to.

Our consultants hold relevant, current UK Security Clearances to enable them to work on sensitive projects for customers within the defence sector and Critical National Infrastructure (CNI).

AMR CyberSecurity has extensive experience providing assurance assessments for clients across different industries, including:

- Completing ‘prepare and control’ framework assessments for new and in-service projects
- Proposing prioritised remediation plans to attain assurance/accreditation
- Supporting Secure by Design, architecture workshops and reviews in accordance with SbD principles, and relevant NCSC guidelines, such as NCSC Zero Trust and cross-domain principles.