UK SPACE AGENCY

SbD Resources Workshop

Introduction

This workshop is designed to walk through the three main Secure By Design (SbD) supporting resources found on the gov.uk SbD portal and explain what they are used for. These tools are:

- Security Controls Taxonomy
  - Example-Secure-by-Design-Controls-Taxonomy-ALPHA.xlsx
- RACI Matrix
  - Cyber-security-roles-and-responsibilities-RACI-matrix-EXAMPLE.xlsx
- Self Assessment Tracker
  - Secure_by_Design_Self_Assessment_Tracker_alpha.xlsx

The Senior Responsible Officer (SRO)

- The official description:
  - As set out by JSP 440 Leaflet 5C, it is the duty or the SRO to ensure Delivery Teams (DTs) are following Secure by Design (SbD) policy, ensure cyber risk is defined and published for the DT, and ensure that cyber risks are actively managed throughout the capability life cycle. The SRO must ensure delivery is underpinned by formal risk management framework.
- What this means:
  - The SRO is the person responsible for signing off on risk
  - The SRO should have an agreed risk appetite, and review if expected risk changes
  - All Security Working Group (SyWG) decisions should be signed off by the SRO (or SRO representative)
  - The SRO should be the last sign-off for security documentation

Note: the SRO does not need to be cyber qualified

Security Controls Taxonomy

When building a digital service, you should leverage appropriate security control frameworks as a blueprint to select controls from as part of security risk management.

Your organisation may already have preferred security control frameworks which should be used across digital services.

The taxonomy aims to help project teams select appropriate security controls from recognised industry security standards and frameworks as part of risk mitigation activities.

It's mapped to Cyber Assessment Framework (CAF) outcomes in order to support organisations with demonstrating their achievement of their respective CAF profile (GovAssure).

The Security Controls Taxonomy template shows how project teams select these frameworks.

Example-Secure-by-Design-Controls-Taxonomy-ALPHA.xlsx

Scenario Company: Ping Floyd

Company Overview:

- Team Size: 15–25 personnel
- Project – Keep Talking: Satellite communications via CubeSat constellation
- Fleet: 5 CubeSat payloads, each contributing 20% of total service functionality
- Mission: Deliver modular, resilient, and secure satcom services
- Sector Ambition: Expanding into defence and tactical communications markets

Differentiators:

- Distributed Architecture: No single point of failure
- Agile & Scalable: Rapid deployment and mission flexibility
- Defence-Ready: Built with security, redundancy, and reliability in mind

RACI Matrix

To effectively embed cyber security within the delivery of government services, project teams need to make security everyone's responsibility. Agreeing team and stakeholder responsibilities will allow you to:

Assign ownership of specific security activities

Identify skills required within the team, and fill any resource gaps with recruitment or training

Give individuals involved in the project personal responsibility for mitigating risk

This should be conducted at the start of the project, with changes in requirements continually assessed as delivery progresses through various phases.

Delivery teams can use this RACI Matrix template as a starting point for assigning roles and responsibilities to Secure by Design activities.

Self Assessment Tracker

Supports the project team to track its progress against the Secure by Design principles and activities in order to deliver appropriate security protections within new systems at each stage of the delivery cycle.

Used to generate an overall SbD confidence profile that is used as input to the Digital and Technology spend control approval process.

In each of the phase worksheets (Discovery, Alpha, Private beta and Public beta or live), you'll see a list of questions associated with recommended Secure by Design activities.

The questions help track your progress through activities and each activity helps you meet one or more of the Secure by Design principles.

You'll complete the tracker during delivery by providing a response to each question, selecting from **Yes**, **No** or **N/A** (not applicable).

Secure_by_Design_Self_Assessment_Tracker_alpha.xlsx

Any Questions?