DIGI GOV EXPO '24

CYBER SECURITY THEATRE

THEATRE SPONSORED BY

CLOUDFLARE

Implementing Secure by Design Across Central Government

Fotini Tsekmezoglou

Head of Securing Digital Transformation

Central Digital and Data Office (CDDO)

DigiGov Expo

DIGIGOVEXPO

Government
Digital & Data

Implementing Secure by Design across central government

Fotini Tsekmezoglou

Agenda

- Strategic context
- Overview of the approach
- Progress (achievements, challenges, immediate goals)
- Working with the industry
- Q&A

The Secure by Design mandate

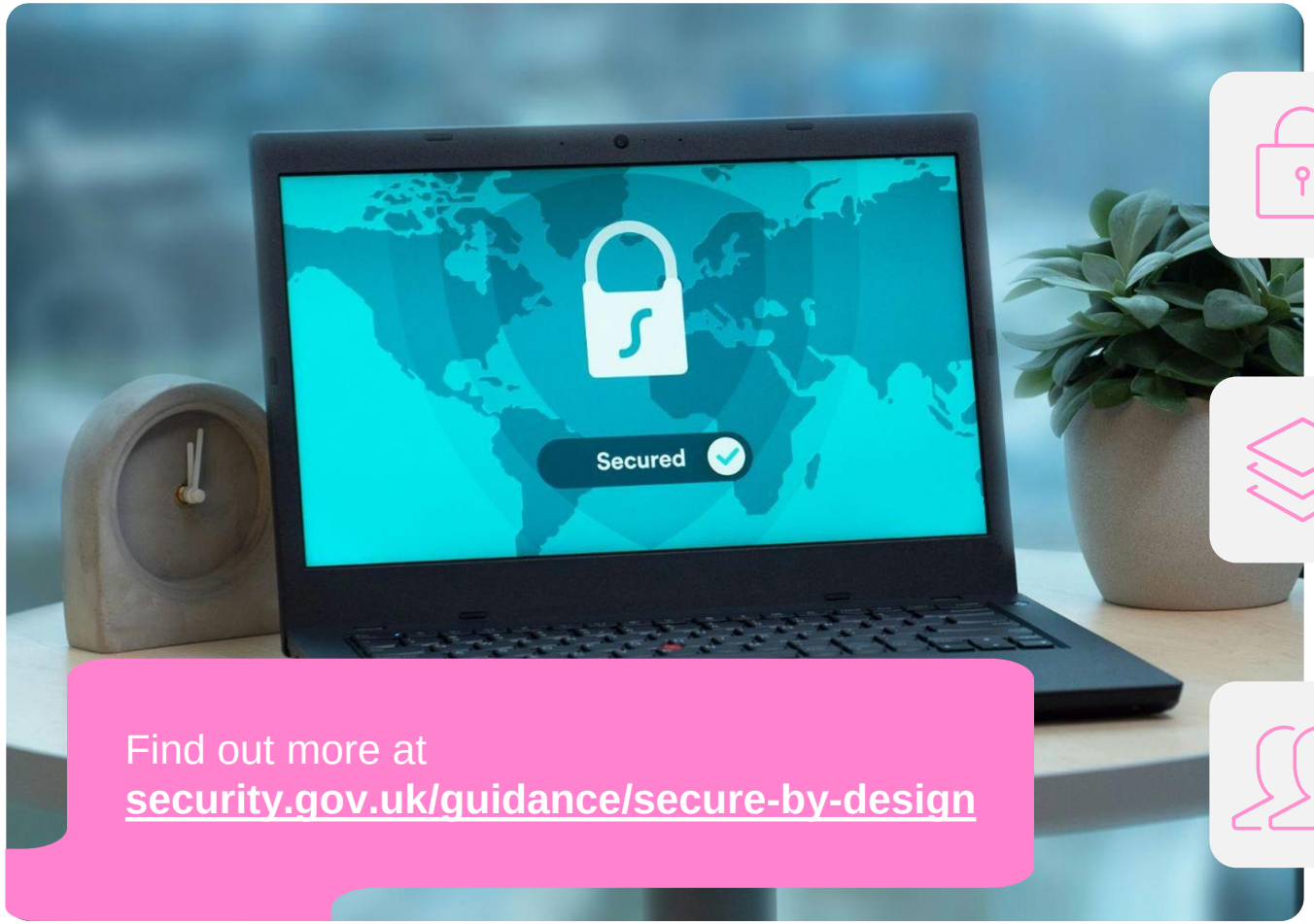
Outcome 9 of the **Government Cyber Security Strategy**

“...ensure that appropriate and proportionate cyber security measures are embedded within the technology government uses, and that the security of digital services is continually assured throughout their lifecycle.”

Commitment 11 of the **Roadmap for digital and data, 2022 to 2025**

“All new services shall comply with the common approach to Secure By Design”

About Secure by Design



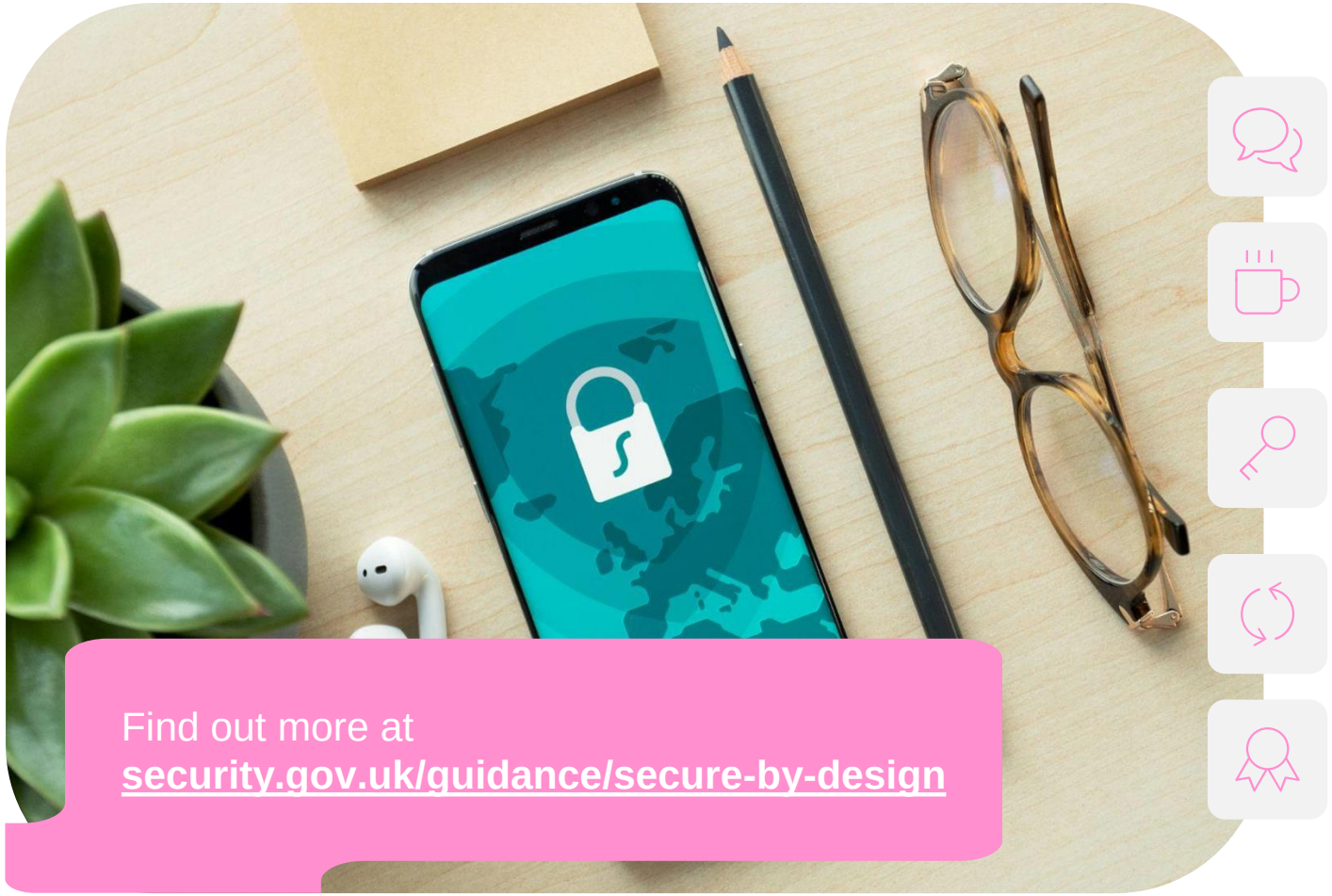
Find out more at
security.gov.uk/guidance/secure-by-design

Improves cyber resilience across government organisations

Incorporates **cyber security practices throughout the digital delivery lifecycle**

Highlights cyber security risks as business risks and makes **security everyone's responsibility**

The benefits



Find out more at
security.gov.uk/guidance/secure-by-design

Increases collaboration between security and delivery teams

Creates a **positive security culture** and upskills non-security teams

Promotes the use of **appropriate and proportionate** security controls

Shifts focus from point-in-time assurance to **continuous security**

Helps organisations **achieve Cyber Assurance Framework outcomes**

Developed in collaboration with

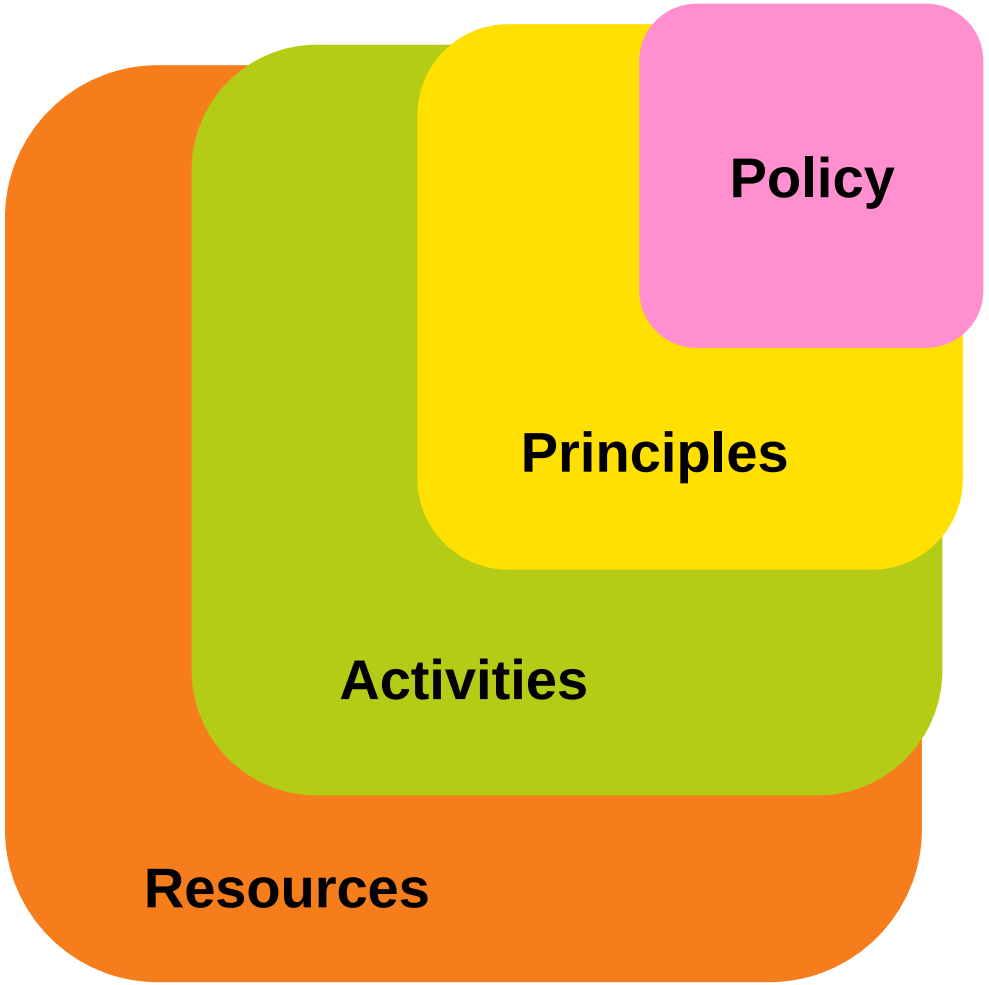
a cross-government working group

Home Office
Department for Education
Driver & Vehicle Licensing Agency
National Cyber Security Centre
Government Digital Service
Driver & Vehicle Standards Agency
Department for Work & Pensions
Ministry of Justice
Cabinet Office
Department for Environment Food & Rural Affairs
Department for International Trade
Northern Ireland Office
HM Revenue & Customs
HM Courts & Tribunals Service
Ministry of Defence
GCHQ
Office for National Statistics
Police Digital Service
Met Office
SLC Student Loans Company
ONR Office for Nuclear Regulation

and industry partners

The approach

Key elements



Mandatory

Monitored via the Cabinet Office digital and technology spend control process and, once new systems services are live, GovAssure.

Recommended

To be adapted by organisations to reflect their internal structure, processes, governance, culture and resources.

The policy

*“All **central government departments and arm’s-length bodies (ALBs)** shall incorporate effective security practices based on the common government Secure by Design principles when delivering and building **digital services and technical infrastructure**.”* Secure by Design Policy

✓

In scope

New projects and services (and those going through major changes) that are passing through the Cabinet Office digital and technology spend control process.

✗

Not in scope

Digital services that are already in operation or undergoing routine maintenance.

The principles

Read more on security.gov.uk

1. Create responsibility for cyber security risk
2. Source secure technology products
3. Adopt a risk-driven approach
4. Design usable security controls
5. Build in detect and respond security
6. Design flexible architectures
7. Minimise the attack surface
8. Defend in depth
9. Embed continuous assurance
10. Make changes securely

The activities

Read more on security.gov.uk

Prepare a secure service

- Agreeing roles and responsibilities
- Identifying security resources
- Considering security within the business case
- Working out the project's security risk appetite
- Tracking Secure by Design progress

Manage your security risks

- Agreeing a security controls set for your service
- Performing a security risk assessment
- Responding to and mitigating security risks
- Assessing the effectiveness of security controls
- Sourcing a threat assessment
- Assessing the importance of service assets
- Documenting service assets
- Performing threat modelling

Maintain continuous assurance

- Evaluating the security impact of changes
- Retiring service components securely

Understand the security landscape

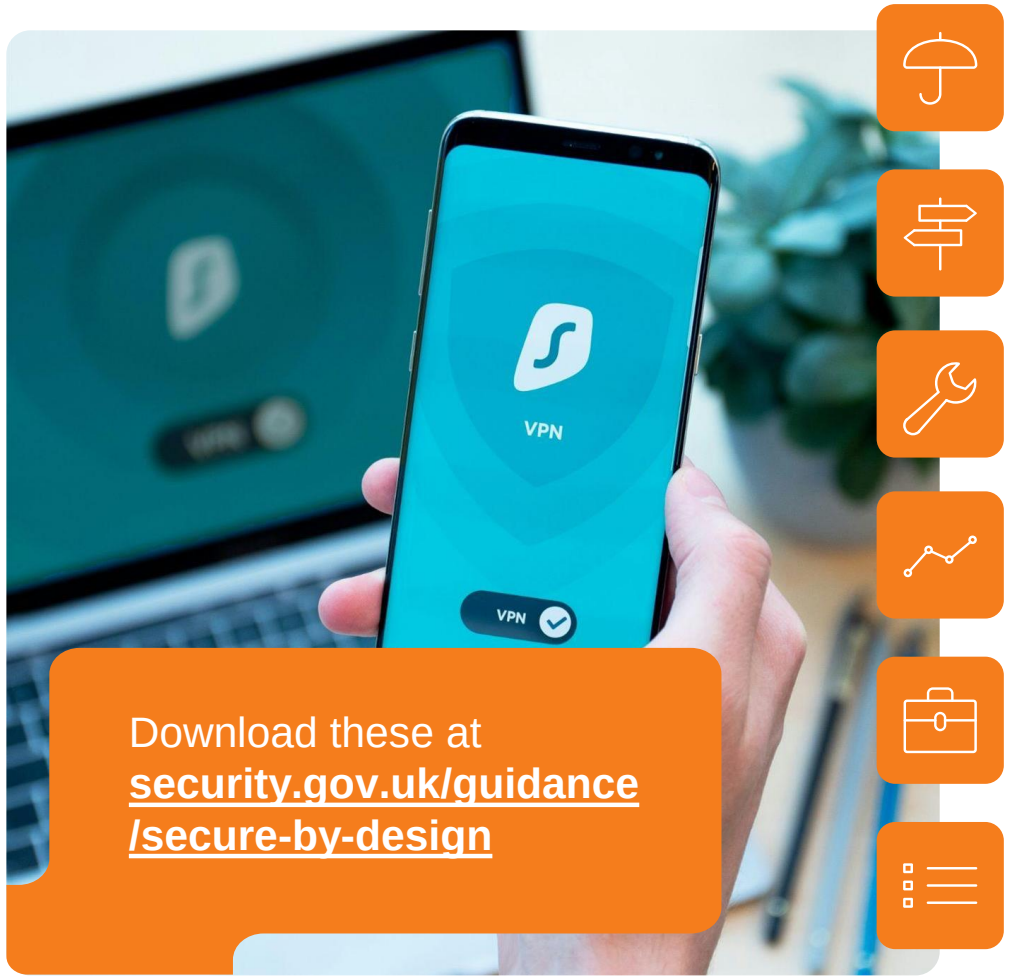
- Managing third-party product security risks
- Understanding business objectives and user needs
- Understanding cyber security obligations

Anticipate and respond to vulnerabilities

- Implementing a vulnerability management process
- Managing observability
- Discovering vulnerabilities

Includes resource

The resources



Preparation Checklist - download
See which requirements your organisation is meeting

Guide to adopting Secure by Design - view
Suggested activities to support implementation

Comms Toolkit - view
Resources to help you inform and engage teams

Self Assessment Tracker - download
Monitor project progress towards meeting principles

Example RACI Matrix - download
See which roles should be involved in each activity

Security Controls Taxonomy - download
Industry security standards mapped to CAF outcomes

Roles and responsibilities

Secure by Design for senior leaders

- Raising awareness, and promoting the benefits, of Secure by Design
- Setting the direction for updating processes, policies, standards and governance
- Establishing Secure by Design as a shared responsibility across functions (not just Security)
- Helping teams to understand their role

CDIOs

Integration into the digital strategy and instilling a security conscious culture.

Adding Secure by Design into policies and practices.

CTOs

Making Secure by Design a key component of service delivery.

Actively supporting delivery teams with technical guidance.

CISOs

Cultivating a positive security culture across the organisation.

Ensuring cyber security SMEs continuously engage with project delivery teams.

SROs

Ensuring Secure by Design is implemented within digital delivery.

Accountable for risk management decisions and direction.

Who Secure by Design affects

Encouraging everyone involved in digital delivery to prioritise security risk management.

Digital & Data

Developers

DevOps

DevSecOps

Technical architects

Project Delivery

System owners / Product owners

Delivery managers

Business analysts

User researchers

Security

Security advisers

Technical security assurance experts

Security risk managers

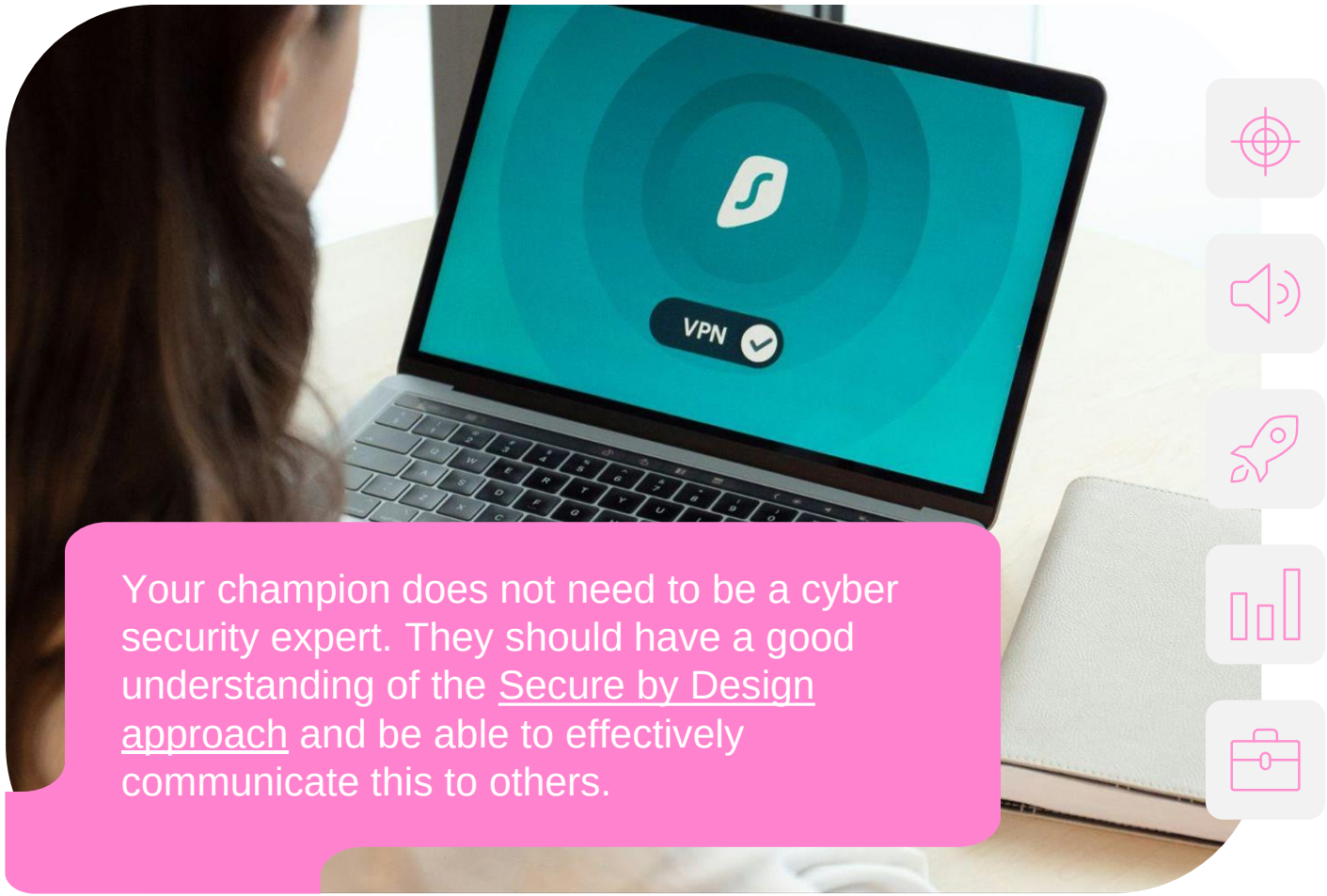
Security architects

Commercial

Commercial Specialist

Procurement Specialist

Your Secure by Design champion(s)



Your champion does not need to be a cyber security expert. They should have a good understanding of the Secure by Design approach and be able to effectively communicate this to others.

- A central point of contact
- Promotes the importance of Secure by Design within their organisation
- Drives development and delivery of a transition plan
- Reports progress to senior leaders and governance forums
- Establishes and runs a Secure by Design working group

Your Secure by Design working group

Made up of representatives from teams affected by Secure by Design including digital and data, project delivery, cyber security, risk management, assurance and commercial.

- Helping to deliver the Secure by Design transition plan
- Encouraging collaboration and knowledge sharing
- Creating alignment between Secure by Design and organisational goals
- Establishing accountability by defining roles and responsibilities
- Addressing any issues that arise during implementation

Implementation

Implementation phases and timescales

Group 1

Ministerial departments, ALBs managing government Critical National Infrastructure (CNI) and organisations managing priority government services.

Preparation
4 months

Transition
5 months

Operation
A conditional extension to Mar 2025 may be granted to some organisations.

2024 Jan Apr Aug **2025** Jan Jul **2026** Jan

Secure by Design commitment deadline

Preparation
6 months

Transition
6 months

Operation

Group 2

All remaining ALBs and other central government organisations (such as executive agencies and Treasury funded regulators). These organisations may move faster should they choose to.

Challenges

- Government = large, complex, and diverse
- Cultural change, security is everyone’s responsibility
- Skills shortage
- Budget constraints
- Other competing priorities (GovAssure)

Working with the suppliers

- Collaborating with the Industry Panel
  - Secure by Design approach
  - Security Schedules and Security Management Plan in Commercial Contracts

- Stay connected
  - Familiarise yourselves with the Secure by Design Approach and send us your comments
  - Secure by Design Newsletter - sign up for these regular updates
  - Briefings at events
  - Blogs

Wrap up

- Aims to **solve a common problem once** so that others won’t have to reinvent the wheel.
- CDIOs will be accountable but security is everyone’s responsibility
- This is **not** one size fits all
- Nobody says it will be perfect from day one. It will be a journey!

Stay in touch

Email us at:
secure-by-design@digital.cabinet-office.gov.uk

Check out the Secure by Design web pages:
https://www.security.gov.uk/guidance/secure-by-design/

Read the CDDO Secure by Design blogs:
https://cddo.blog.gov.uk/?s=secure+by+design

Sign up for Secure by Design newsletter here