



What is Secure by Design?

An approach to **incorporate cyber security practices into digital delivery from the start and consistently** throughout the service lifecycle.

A way to increase cyber resilience across central government organisations by building **risk-driven cyber security** into digital services.

An approach that highlights cyber security risks as delivery and business risks, **making risk management everyone's responsibility** across a delivery team.

A policy that is mandatory for projects required to pass through the **digital and technology spend controls approval process** and recommended for others.

Secure by Design is

- ✓ mandatory for central government departments and arm's length bodies (and optional for other public sector organisations)
- ✓ an approach with mandatory principles, and best practice activities with supporting tools
- ✓ monitored through existing assurance processes, including the digital and technology spend controls approval process
- ✓ designed to drive effective collaboration between delivery teams, security experts and colleagues in other roles

Secure by Design is not

- ✗ a tick box exercise - it requires a significant culture change where security is considered throughout digital delivery
- ✗ an assurance process - though it contributes towards achieving the government Cyber Assessment Framework (CAF) profiles as part of GovAssure
- ✗ something purely for security professionals - it impacts everyone involved in digital delivery, including delivery teams, project management and procurement

Visit the Government Security website's [Secure by Design pages](#) for:

- the Secure by Design policy, which sets out the scope of the approach
- the Secure by Design principles, reflecting typical security challenges in digital delivery faced by government organisations
- best practice activities and resources that can be tailored by delivery teams to help them meet the principles during the digital delivery lifecycle
- templates and tools to help organisations assign security responsibilities, identify appropriate security controls and track progress towards meeting policy requirements