



Cyber Security- Secure By Design and Architecture

G-Cloud 15 Framework
Lot 3 Cloud Support: Service Definition

January 2026

Contents

[Service overview](#)

[Our service in action](#)

[Our methods and technical expertise](#)

[Case studies](#)

[Why choose us?](#)

[About AtkinsRéalis](#)

[Contact us](#)



Service overview

AtkinsRéalis Secure by Design (SbD) service embeds a proportionate and people focused security culture, alongside proven governance frameworks and security standards, to pragmatically reduce your operational cyber risks. We design security as an enabler – **protecting equipment, citizens, operations and missions** that is based on quantifiable likelihood and operational impact.

Benefits include:

- Designed-in security across discovery, design, build, commission and operations to avoid late-stage rework.
- Outcome-based assurance mapped to UK Service Standard point 9 and the National Cyber Security Centre (NCSC) Cyber Assessment Framework (CAF).
- Reusable security architecture patterns and secure defaults that accelerate safe delivery.



Our service in action

We work alongside your delivery and ops teams to make security **visible, usable and testable**. The service is tailored to your governance and risk appetite so that the right controls are built once and operated every day.

- Operational context capture and risk ownership established from day one.
- Threat modelling and risk assessment iterated at each lifecycle stage to guide design choices.
- Secure-by-default technology selection and third-party due diligence to manage supply-chain risk.
- User-centred security processes, run-books and guardrails that teams adopt in practice.

Our methods and technical expertise

Our architects and engineers combine modern architecture practice with recognised frameworks, so you gain practical security that **aligns to policy and regulation without slowing delivery.**

- Security architecture for cloud, hybrid, IT and Operational Technology (OT) environments with Zero Trust principles and segmentation.
- Secure cloud landing zones and guardrails for Azure, Amazon Web Services (AWS) and Google Cloud Platform (GCP) covering identity, encryption, logging and resilience.
- Design for observability, backup and recovery so security and continuity are proven before go-live.
- Outcome-based assurance producing traceable artefacts from requirements → design → test → operate, aligned to Service Standard and NCSC CAF.
- Use of TOGAF/ADM, NIST 800-53/CSF, ISO 27001, and JSP mappings where relevant.



Why choose us? – trusted results, proven impact



We bring **high-performing, multi-disciplinary teams** who have delivered Secure by Design at national scale. Our blend of cyber engineering, architecture and domain expertise turns policy into working security that delivery teams adopt.

- Proven at scale: SbD embedded across 300+ Defence capabilities and adopted as RAF best practice.
- Pragmatic delivery in regulated environments – Defence, CNI and government.
- Clear evidence trails that satisfy sponsors and auditors without slowing delivery.

Case studies

Find out how our impact is demonstrated
through real-world delivery

CASE STUDY

Ministry of Defence

RAF adoption of SbD as a gold standard

We embedded SbD across major programmes, enabling teams to capture, communicate and remediate risks at all classifications. This improved compliance with JSP 440/Leaflet 5C and JSP 453, streamlined accreditation/audit readiness, and built enduring stakeholder trust.

- Scope: AIRSEEKER; PHOENIX 3 Fleet Tracking; NSoIT/OpNET; Multi-Role Support Ship; FADS T83/T91 & RADAR; Protector RPAS; C17/CSAT/CX130; SHIPS OC; MCS UEW/CSA/MEWT/FWCMS.



- faster, fewer-surprise approvals
- sustained security posture post-deployment.



CASE STUDY

MOD cyber mission data (CMD)

As lead partner for data collection and product design, we applied Agile/Scrum across rainbow teams to deliver intelligence APIs and high-impact visualisations that increased cyber resilience across the estate. The work was recognised with a Defence board commendation.

- Approach: user-centred product design, iterative assurance, and integrated SbD controls.



- Accelerated delivery cadence.
- Clearer mission outcomes
- Strengthened cyber resilience.



CASE STUDY

Threat hunting business architecture

Using a TOGAF-based approach and NCSC guidance, we produced decision-ready business architecture and options analysis to guide investment prioritisation for the MOD's future threat hunting capability.



- Investment clarity
- Traceable requirements
- Blueprint for capability development



About AtkinsRéalis

AtkinsRéalis is a global leader in engineering, design, and digital services, renowned for delivering end-to-end solutions across government, infrastructure, energy, transportation, and technology sectors.

Founded in 1911, our company operates in over 160 countries with a workforce of more than 36,000 professionals, combining deep technical expertise with cutting-edge digital innovation. Notable for internationally recognised engineering projects such as the Burj Al Arab, the Ho Chi Minh City Skyscraper and the Elizabeth Line, alongside digital projects for MoD, HMRC, National Highways and Heathrow, we have earned a reputation for consistently delivering high-quality work.

Our digital capabilities span business strategy, architecture, design, implementation, project management, and lifecycle support, leveraging advanced technologies such as AI, digital twins, and data-driven systems to transform government, infrastructure and energy systems worldwide. With our strong focus on human-centric design, resilience, and sustainability, AtkinsRéalis is a trusted partner for complex, mission-critical projects for clients across government, defence, infrastructure and beyond.



CONTACT US



ccs@atkinsrealis.com



Nova North,
11 Bressenden Place,
Westminster, London,
SW1E 5BY