

# AI Governance AI Security

For Cloud

G-Cloud 15

Service Definition

2026

**Security. Risk. Resilience.**



# Contents

About Us **03-04**  
Service Capabilities

---

Service Description **05**

---

AI Security **06**  
AI Governance

---

What We Deliver **07**

---

Assurance **08**

---

How We Deliver **09**

---

Case Studies **10-11**

---

Service **12-13**  
Information

---

# About Us

---

Hampden Consultancy Group (HCG) supports public sector and regulated organisations make security clear, practical, and resilient. HCG embed into delivery teams and organisations, doing the specialist security delivery so organisations can move at pace whilst also proactively managing risk and achieving a mature governance structure.

HCG have supported delivery and security teams across government and critical national infrastructure, from local authorities to central government departments, ensuring our clients meet scrutiny from leaders, auditors, and regulators with confidence.

## How We Work

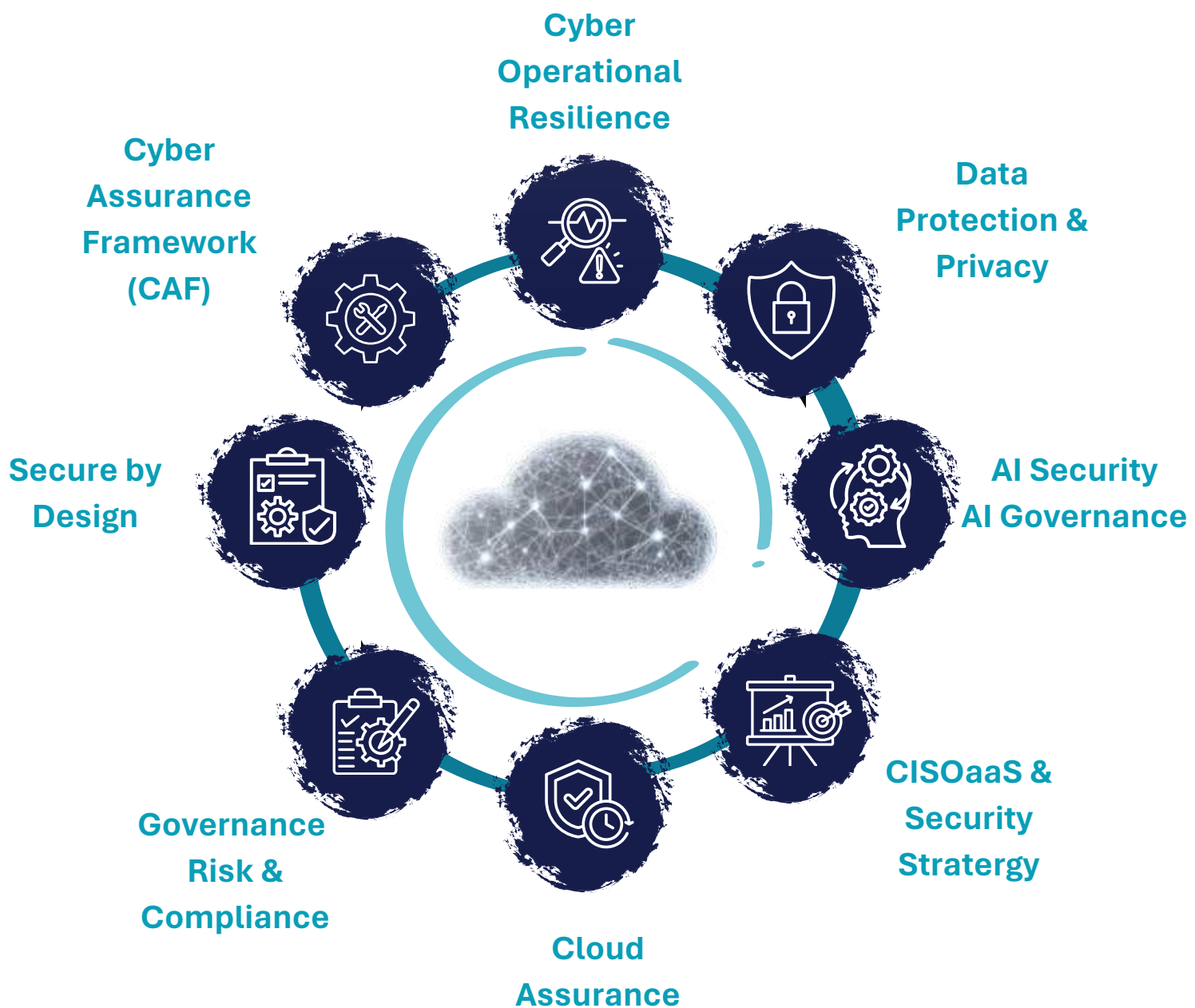
HCG embed into your delivery rhythm to become efficient and aligned to the business objectives. Communication is clear and concise, in line with your organisation's presentation and communication policies or frameworks.

## What To Expect

We endeavour to add value throughout and provide consultancy through clear documentation along with contributing to organisational artefacts. We evidence our deliverables, in line with current governance, industry best practice, the relevant regulations along with academic rigour where appropriate.



# Our G-Cloud Service Capabilities



# AI Governance & Security

## Service Description

HCG establishes AI governance for cloud services: roles, thresholds, decision points, ethics, controls and evidence. We help teams adopt AI responsibly with clear accountability, proportionate assurance and workable processes that fit delivery. AI security controls are implemented with direct links to risk management and client's risk appetite.

We also support assurance and compliance workflows (including data protection impact considerations), Secure by Design within AI and supplier assurance, so AI use is secure, resilient and assured.

## Who It's For

Organisations, programmes and projects adopting AI with the public sector or regulated organisations.

## Features

AI inventory, ownership model and decision thresholds and security controls.

Governance cadence and reporting aligned to leadership needs.

Policies/standards for AI use, procurement and third parties.

Risk management workflow and decision logging.

Assurance checkpoints across design, build, deploy and change.

Evidence pack structure and improvement roadmap.

## Benefits

Clear accountability for AI decisions and risks.

Reduced assurance and reputational exposure.

Faster decisions through defined thresholds.

Assured, government aligned evidence.

Better procurement outcomes through clearer requirements.

Sustainable governance that drives the foundations of responsible AI employment.

# AI Security

# AI Governance

**Adopt** AI securely, responsibly and with confidence

AI adoption is accelerating across government and regulated industries. Regulators, auditors, and oversight bodies now expect organisations to prove that AI is being deployed securely, responsibly, and in line with policy. The challenge is balancing innovation with governance and appropriate risk management, subsequent security controls and assurance.

HCG assists organisations bridge that gap. We design governance frameworks, risk models, and practical application that allow delivery teams to use AI while giving boards and regulators confidence that risks are being identified and subsequently mitigated appropriately.

## What We Do

- ✓ AI governance frameworks tailored to organisational risk appetite and sector requirements.
- ✓ Risk triage for AI use cases, from pilots to enterprise rollouts.
- ✓ Risk assessment and management frameworks built for AI adoption and assurance.
- ✓ Risk-linked mitigating control sets for data, models and suppliers.
- ✓ 'Safe use' patterns that delivery teams can apply immediately.

## Outcomes

- 🎯 Innovation that remains assured and secure.
- 🎯 Clear accountability and clarity for AI decisions.
- 🎯 Confidence for boards, regulators & oversight bodies.
- 🎯 Reduced risk of legal, reputational or operational impact.



# Assurance

Objective evidence for boards, regulators & stakeholders

Independent assurance provides decision-makers with confidence that security, risk and compliance are being managed and implemented effectively. It demonstrates that controls are in place, governance is aligned and critical services can withstand scrutiny from regulators, auditors and boards.

HCG delivers assurance across government, public bodies and regulated industries. Our consultants bring experience from MOD, central government and CNI, producing evidence that satisfies oversight requirements and enables leaders to make informed decisions.



## What We Deliver

- ✓ **Enterprise assurance** - holistic assessments across policies, controls, and governance.
- ✓ **Programme and project reviews** – assurance at key delivery points.
- ✓ **Supplier assurance** – validate third-party risk and compliance.
- ✓ **Framework assessments** – tailored to your organisation, aligned to CAF, GovAssure, ISO 27001/42001, NIS, and NIST.
- ✓ **Clear remediation roadmaps** – prioritised actions, not generic findings.
- ✓ **Board-ready reporting** – assurance artefacts designed for executives and oversight bodies.

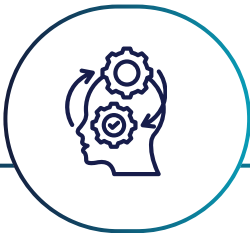
## Outcomes

- 🎯 A complete, transparent risk picture across your organisation.
- 🎯 Fewer surprises during audit, regulatory review, or board challenge.
- 🎯 Evidence that stands up to scrutiny from Cabinet Office, Regulators, ICO or shareholders.
- 🎯 Practical, prioritised fixes that reduce risk fast.



# What We Deliver

We take ownership of the Governance, Risk & Compliance requirements for your cloud programme



## AI governance operating model

Roles, RACI, forums and decision thresholds

Practical policies and standards for AI use

Reporting that leadership can act on



## AI risk & compliance workflow

Risk assessment, decision log and escalation routes

Compliance workflow and evidence expectations

Supplier assurance for models and AI services



## Assurance checkpoints & evidence

Stage gates across design, build, deploy and change

Prioritised improvement plan with owners and milestones



## Capability transfer

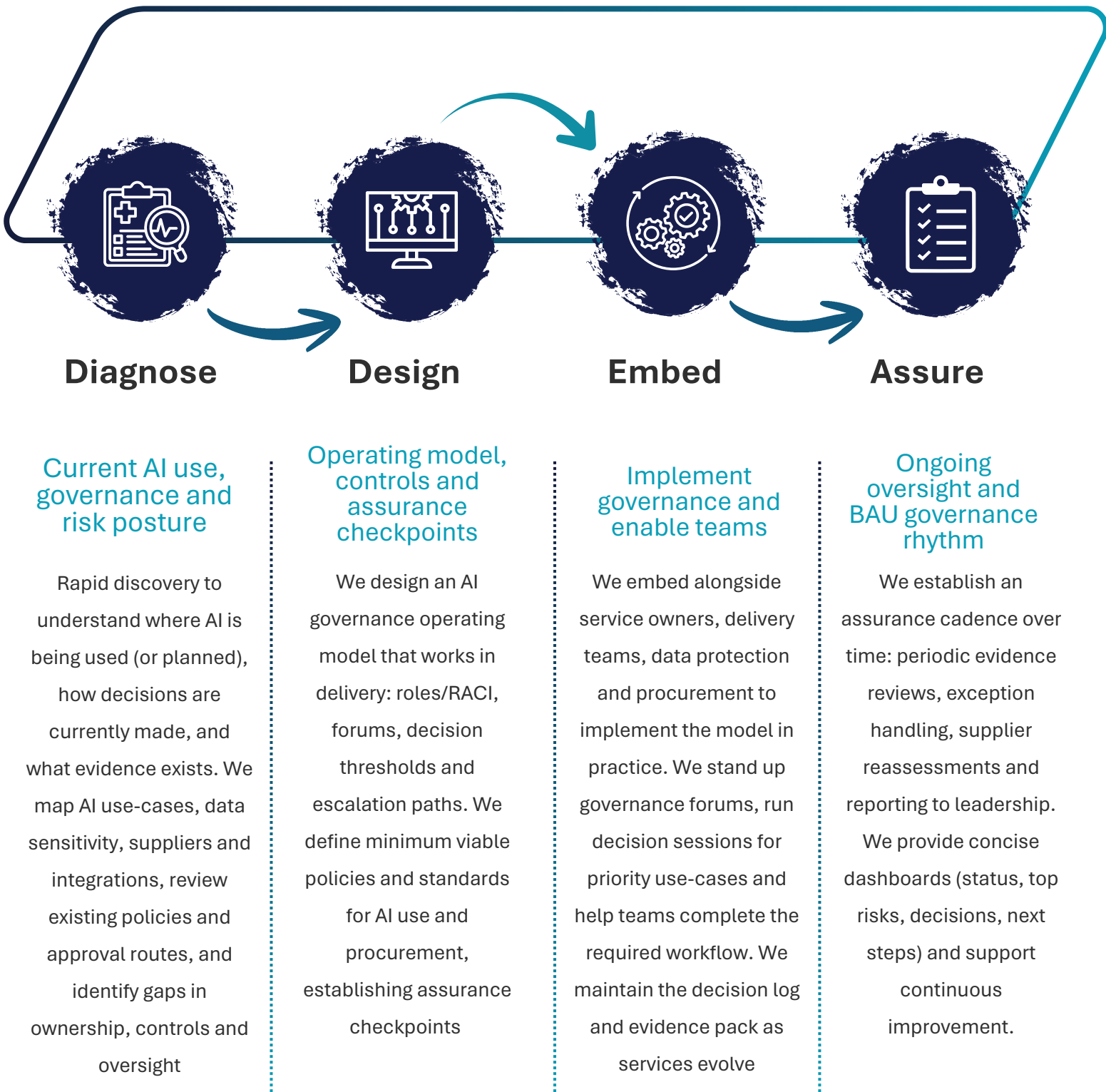
Playbooks and templates teams can reuse

Coaching for service owners and delivery teams

Handover into BAU governance cadence

# How We Deliver

We deliver end-to-end, or as standalone work packages to fit your need and pace



# Case Study



Department  
for Transport

## The Challenge

DfT needed to turn the mandated cross-government Secure by Design requirement into an enduring, risk-driven model that could embed and scale across digital projects and programmes

However, tight deadlines, limited SbD-skillset, and fragmented assurance practices created friction and risked non-compliance with the Government Digital Service (GDS) mandate

Compounding this was inconsistent delivery maturity, unclear roles and responsibilities, convoluted risk ownership and management, and the complexity of embedding SbD across a diverse supplier ecosystem



### Objectives

Meet the SbD mandate on time and in full adherence, embedding SbD across DfT projects and programmes

Strengthen governance and reporting to give leadership clear visibility of risk, progress, and assurance

Enable self-serve adoption with tooling, artefacts, and guiding DfT towards best practice, reducing reliance on specialists



### Our Approach

Tailored SbD policy and governance model aligned to DfT delivery

Project-ready artefacts for efficient and consistent evidence

Self-serve portal and communication to scale adoption and ease pressure on delivery teams

Lifecycle assurance framework mapped to CAF/GovAssure



### Impact

SbD successfully implemented and efficiencies harnessed DfT-wide

Greater clarity of risks to the executive team

Supply chain risk management and assurance

Security from the outset

# Case Study



Secure by Design Technical Lead Support for Defence Science and Technology Laboratory (Dstl)

## The Challenge

Dstl was tasked with delivering a novel technology programme in a protected MOD environment, where security and assurance requirements are exceptionally high. The project needed to meet both Dstl's and the Senior Responsible Owner's (SRO) security expectations, align with the partnered DE&S assurance standards, and be fully prepared for MOD Cyber Defence & Risk (CyDR) 2nd Line Assurance inspection. The challenge was to embed Secure by Design (SbD) from the outset, ensuring robust evidence and governance, rather than relying on late-stage fixes or retrospective paperwork



### Objectives

To ensure the programme met MOD policy (JSP 440 Leaflet 5C) by integrating security into every stage of delivery, maintaining up-to-date security records and decision-making, and achieving 2LA readiness for CyDR inspection.

The goal was to provide senior stakeholders with confidence that security was being managed proactively and could withstand scrutiny



### Our Approach

Assessed the programme's current security position and identified key gaps against MOD SbD (JSP 440/CAAT).

Produced a clear, prioritised roadmap to address assurance requirements

Strengthened governance and documentation to satisfy SRO and DE&S scrutiny

Set up security working groups and delivered essential SbD artefacts

Readied the programme for 2nd Line Assurance with structured evidence and ongoing support



### Impact

The programme moved from "security accreditation chasing delivery" to a clear, repeatable Secure by Design approach.

Security was embedded earlier in the lifecycle, governance was strengthened and assurance readiness was demonstrably improved against JSP 440 Leaflet 5C and senior stakeholder expectations

Dstl's project is now positioned to operate securely, with robust evidence and governance supporting MOD assurance and future capability growth

# Who we've worked with



## Why Trust Us?



info@hampdencg.com



Hampden Consultancy Group



www.hampdencg.com

# Service

# Information

As a specialist SME, we're agile, adaptable, and focussed on our clients' success. We blend technical assurance, governance and delivery expertise to solve complex security challenges for public & regulated sector organisations. Our collaborative approach delivers tailored outcomes and real change, making security practical, sustainable, and aligned to your mission

## Onboarding & Offboarding

---

We provide a smooth onboarding process, including a kick-off workshop, stakeholder mapping, and access to all relevant artefacts and templates. Our team works collaboratively with yours from day one, building strong relationships and ensuring knowledge transfer. At project close, we deliver a comprehensive handover pack, including evidence, recommendations, and a close-out meeting to ensure continuity

## Contract Management

---

Our contracts are transparent and flexible, with clear Statements of Work and pricing models (Time & Materials or Fixed Price) agreed up front. A dedicated engagement lead supports you throughout, ensuring deliverables are met to the highest standard and adapting quickly to changing needs

## Project Management

---

We use an agile approach, with regular progress updates, milestone tracking, and stakeholder engagement. Weekly reports and review meetings keep you informed, and our team is proactive in identifying and resolving issues. For longer-term engagements, we work with you to plan resource needs and delivery pipelines in advance

## Risk Management & Quality

---

Risk is managed continuously through proactive management and open communication. We provide regular risk reviews, mitigation strategies and strategic recommendations. Our quality management system is aligned to ISO9001 and ISO27001, with robust checks and feedback loops to ensure deliverables meet your requirements

## Security & Clearances

---

All information is handled securely in line with both The UK Government Security Classification Policy and industry standards. Our consultants are security cleared (BPSS/SC/DV as required), and we maintain strict controls over data, access, and confidentiality. We are Cyber Essentials Plus and ISO27001 & ISO9001 certified



[www.hampdencg.com](http://www.hampdencg.com)

2026