Hampden Consultancy Group

Governance Risk Compliance

G-Cloud 15

Service Definition

2026

Security. **R**isk. **R**esilience.

Contents

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.

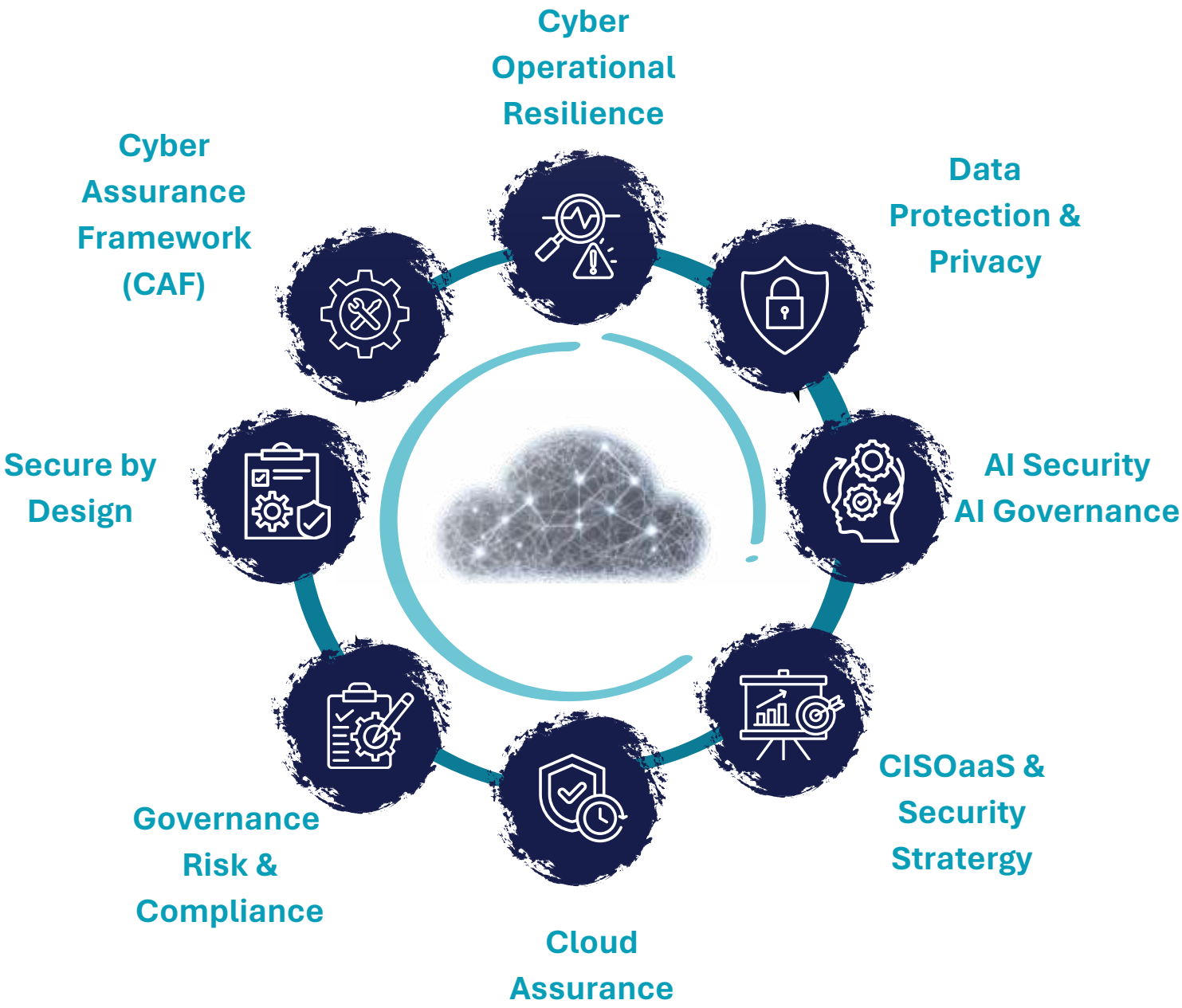
How We Work

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



Governance Risk & Compliance

Service Description

HCG provides Governance, Risk & Compliance (GRC) support for cloud services, from digital transformation and organisation governance, from project to organisation risk management, to alignment to Secure by Design, NIST, ISO, NCSC CAF and GovAssure expectations. We baseline maturity, map controls and ownership through a risk-based approach, and establish a governance cadence so risk decisions are timely, recorded and educated.

We build and maintain an assured evidence pack (including a WebCAF-ready structure), strengthen supplier assurance, and convert gaps into a prioritised improvement plan with owners and milestones. The outcome is clearer accountability, faster assurance decisions and sustained compliance from change through to BAU. We drive preparation; independent reviews remain independent.

Who It's For

Public sector and regulated organisations delivering, modernising or operating cloud services that need CAF/GovAssure readiness, clear risk ownership and evidence that stands up to assurance and audit

Features

Baseline CAF/SbD maturity and prioritised gap analysis.

Map controls, ownership and RA(S)CI across services.

Built CAF/SbD-ready evidence pack and maintenance approach.

GovAssure mobilisation and self-assessment support (Stages 1–3).

2nd Line Assurance readiness: evidence walkthroughs and challenge preparation.

Supplier and third-party assurance for cloud and SaaS.

Targeted Improvement Plan and remediation tracking into BAU.

Benefits

Faster assurance decisions and approvals.

Assurance-ready evidence maintained.

Reduced rework by identifying gaps early.

Clear accountability for controls and risks.

Stronger supplier assurance, reduced third-party exposure.

Sustainable governance cadence into BAU.

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 safely, responsibly, and in line with policy. The challenge is balancing innovation with governance and appropriate 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
- DPIA/RA templates 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

An embedded delivery partner

Embed into delivery: planning, design reviews, governance and assurance

Own the GRC workstream plan, actions and dependencies

Coordinate delivery teams and suppliers so assurance enables delivery

CAF/GovAssure evidence pack

Build and maintain a CAF-mapped, WebCAF-ready evidence pack

Keep evidence current as designs and services change

Make assurance traceable: what exists, gaps, owners, due dates

Ongoing assurance

Establish a lightweight assurance cadence across delivery and change

Review evidence quality, control implementation and risk decisions

Prepare services for IARR and audit activity without disruption

Governance & reporting

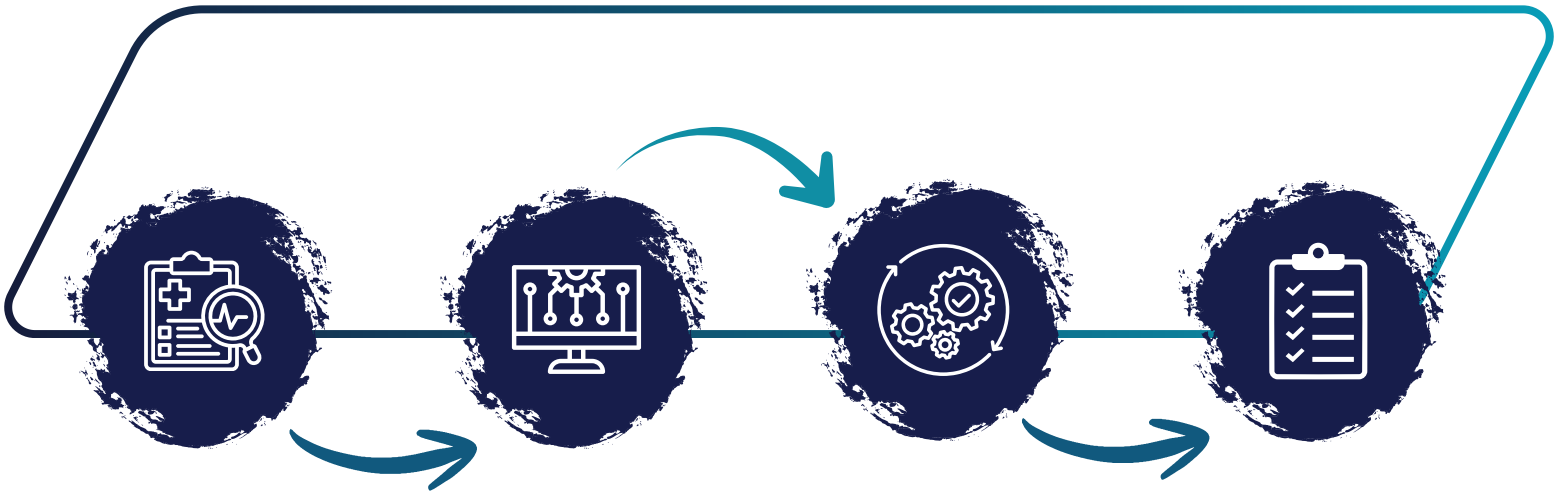
Run governance forums (or integrate with existing cadence)

Provide SRO-ready reporting: status, top risks, decisions, next steps

Support risk owners to make proportionate, recorded decisions

How We Deliver

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



Diagnose

Gap analysis & roadmap

Rapid discovery to understand your cloud service, delivery rhythm and supplier landscape. We review existing artefacts and evidence, run targeted interviews, and baseline maturity against NCSC CAF outcomes and GovAssure expectations. Output: a prioritised roadmap, top risks, and an agreed plan for the next 30/60/90 days

Design

Operating model & artefacts

We design a pragmatic GRC operating model that works in delivery: governance cadence, roles and ownership (RACI), risk decision points, and assurance checkpoints. We define what “good” looks like and build the evidence pack structure so delivery teams and suppliers know what to produce and how it will be assessed

Embed

Embedded GRC delivery

We embed alongside the delivery team and integrate into existing forums and ways of working. We coordinate contributors, maintain and ensure controls and evidence are produced and kept current as designs change. We strengthen supplier assurance and keep the programme moving without GRC becoming an inhibitor

Assure

Ongoing assurance (to meet GovAssure/2LA)

We run an assurance cadence across delivery and change: evidence quality checks, control implementation review, and clear findings with prioritised actions. We prepare teams for GovAssure & 2LA activity and support leaders with concise reporting: status, top risks, decisions and next steps

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?

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

2026