

G-Cloud 15 Service Description

GovAssure (NCSC CAF) Independent Assurance

GovAssure (NCSC CAF) Independent Assurance

GovAssure is the cyber assurance scheme designed by UK Government and National Cyber Security Centre (NCSC) to assess the resilience of HM Government Critical Systems including Critical National Infrastructure (CNI) supporting essential services. The scheme applies to HM Government Departments, Arms-Length Bodies, Operators of Essential Services and Cyber Oversight Bodies ‘Scheme Partners’. The scheme is split into 5 Stages and uses NCSC’s Cyber Assessment Framework (CAF) to standardise the assessment of an organisation’s ability to resist, detect and respond to cyber security threats with progress measured against the Government Cyber Security Standard.

What is the Service

Methods is an NCSC Assured Cyber Consultancy who has been assured to the highest standards as defined by NCSC and professional bodies such as UK Cyber Security Council. With a proven track record of delivering cyber security consultancy expertise, we pride ourselves on working closely with our clients - often augmenting in-house capability.

A Cyber Security Essentials Plus certified company, the services provided by the Cyber Portfolio align with ISO/IEC 20700 family of information security management standards, ensuring work is appropriately scoped, planned and delivered to the highest standards.

Methods provide a holistic approach to the provision of services in support of the GovAssure Scheme with work undertaken by industry qualified Cyber security experts, many holding CCP Lead Practitioner else qualified to Chartered status, able to offer approved GovAssure Independent Assurance provider guidance and support to both public and private sector clients, covering the entirety of the Security organisation.

GovAssure is the new cybersecurity assurance regime from the government, adopting NCSC’s Cyber Assessment Framework (CAF) as its central framework, replacing the cyber security element of the Departmental Security Health Check (DSHC).

Methods is a Non-NCSC Assured GovAssure Independent Assurance Reviewer (Supplier) and will become a NCSC Assured GovAssure Independent Assurance provider later in 2024. We have traditionally specialised in supporting HM Government Departments such as DWP, MoD as well as Local Government and the wider public sector, but have in recent years expanded to Private Sector to include Defence, Energy and Automotive. With a focus on ensuring that IT systems meet specific security requirements and standards, delivered by dedicated SME teams/practices, Methods have the deep knowledge and experience to provide a professional service to our clients.

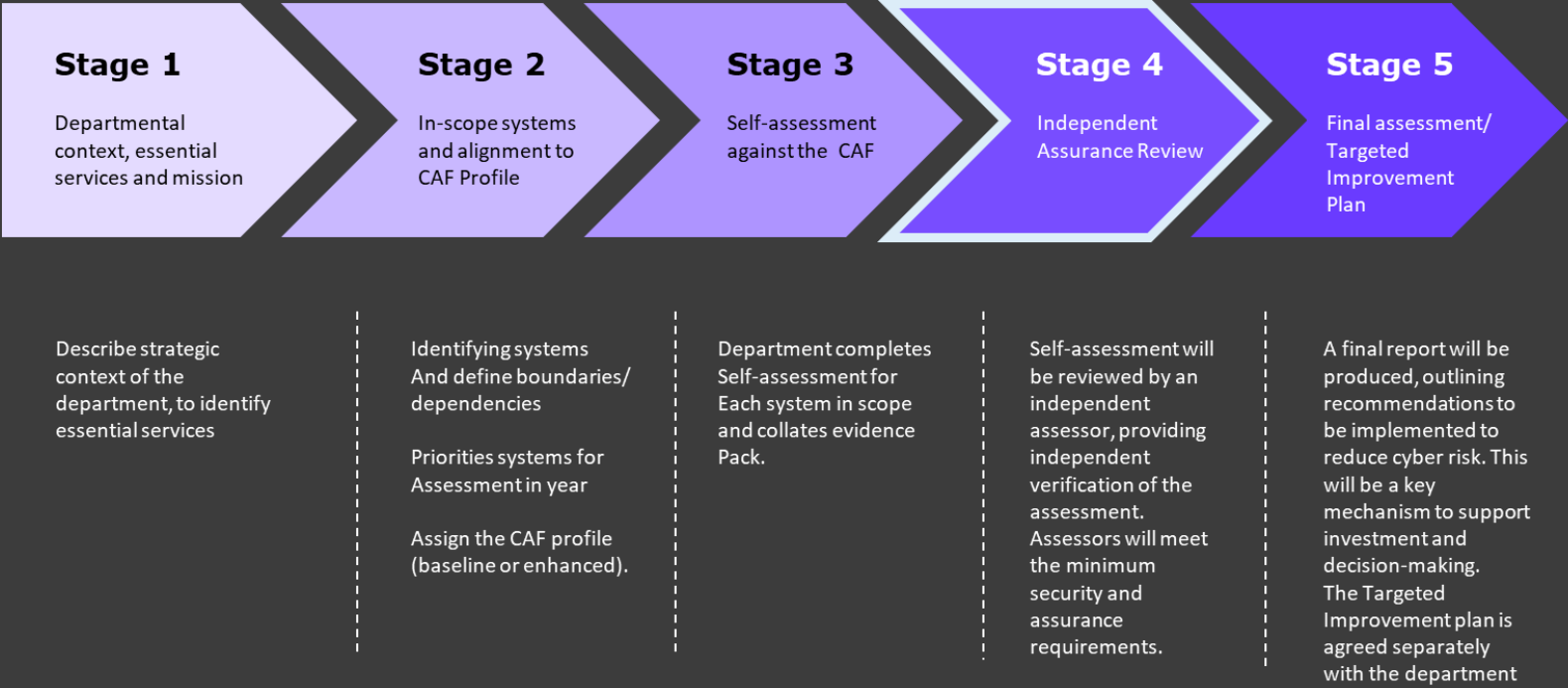
Methods manage engagements in accordance with industry best practice standards and frameworks and meet NCSC requirements for certified professional cyber services companies. Working closely with our clients to ensure that the services we provide have been correctly scoped, planned and delivered securely, as part of “Secure by Design principles”, with our customers interests and needs at the forefront of our thinking.

Methods is a certified cybersecurity consultancy with expertise in NCSC GovAssure CAF for baseline and enhanced profiles. Holding CCP Lead Practitioners and ChCSP endorsements from NCSC and UK Cyber Security Council, delivering approved advice and guidance to a diverse range of clients to help them work towards Government Assurance and Accreditation. In meeting the standard for undertaking GovAssure work, Methods is engaged with NCSC, Cabinet Office and CNI Regulators for the upcoming Cyber Resilience Audit (CRA) scheme to include provision of independent audits to support CNI public and private sectors.

For GovAssure, Methods recognise the need to provide a ‘named authority’ who will provide oversight throughout the review, act both as a point of focus and escalation, and take responsibility for the quality and standard of the work in meeting required standards. Methods will provide a Head Consultant, typically qualified to Chartered status, to act as the Named Authority.

GovAssure end-to-end

GovAssure consists of five main stage:



Methods GovAssure Cyber teams are led by NCSC Trained Head Consultants (Chartered, ChCSP Audit and Assurance) and nominated Lead Auditors (Principal, PriCSP Audit and Assurance). The Head Consultant or Head of Service will act as your immediate point of focus and will lead an experienced Team of qualified Audit and Risk professionals who are:

- steeped in use of National Cyber Security Centre (NCSC) Cyber Assessment Framework (CAF) and the WebCAF Digital Interface
- security cleared to SC or DV with Public and Private sector experience

Methods’ GovAssure Project Sponsor (Chartered, ChCSP Risk Management) will provide additional executive support at Director level. Our Team support, advise and guide in-house teams – building the capabilities needed to meet CAF Objectives, supporting and guiding your teams through Government Guidance for Stages 1-3 and 5.

Our Independent Assurance Review Report and Target Improvement Plan provide in time assessment of your Security posture to include cyber security resilience against rising threats and encapsulating policies, procedures and governance to:

- Pinpoint strengths and weaknesses and/or highlight gaps in your organisation’s cyber security defences across technical infrastructure, architecture and design, governance, policies and procedures and education and awareness against NCSC CAF
- Provide an independent and objective view on the maturity of cyber security controls and countermeasures
- Establish Action Plans to mitigate and address identified weaknesses and vulnerabilities to improve Cyber Resiliency.
- Meet statutory, legal and sector specific industry compliance requirements including GovAssure/CRA Cyber Security Scheme

Contact details

- Enable the setting of meaningful target security levels for organisations to achieve, possibly reflecting a regulator view of appropriate and proportionate security.
- Be as straightforward and cost-effective to apply as possible.

We are particularly interested in the vulnerabilities inherent in the organisation systems, that could lead to the compromise of their confidentiality, integrity, or availability of assets. Our experience consultants ask the simple question “Who would want to exploit this vulnerability, and why?” This facilitates our consultants to study the potential adversaries, their motivations, and their capabilities. Furthermore, Methods look determine whether a given threat source has the means to exploit one or more vulnerabilities to attack the organisation assets.

Our methodology and approach are agile, which is designed to integrate seamlessly into the organisation, complementing and innovating the current working practices. Whether the organisation is looking for ad-hoc support, or a long-term partner, our team of professional, verified and approved by NCSC Cyber Security and UK Cyber Security Council, our experts, with the ability to help identify and implement best and most viable solutions. Aligned with NIST, NCSC, OWASP, and MOD DEFSTAN 05-138 for dynamic security solutions.

One of our core tenets is collaboration, which lays out how our team works with the client. We adopt the principles of openness and knowledge transfer to empower the people and build impressive, sustainable governance around complex multi-cloud solutions. We work closely with key stakeholders and programme teams to devise a bespoke solution that meets the demands of the business processes, strategic business objectives and regulatory requirements. Our consultants have a strong background in both public and private sectors and will quickly adapt to the environment, providing specialist expertise to design innovative and risk-based solutions that meet your specific business needs and outcomes.

We at Methods, provide pragmatic and proportionate risk-based guidance as trusted consultants covering compliance, architecture, and design assurance; system accreditation across Code of Connection (CoCo) and MOD DefCon standards. Our experienced consultants have proficiency working on a variety of Government projects with different divisions including critical national infrastructure (CNI), defence, policing, justice, education, healthcare, border control, central government, local authorities, and government digital services.

In line with HMG requirements, Methods is certified to Cyber Essentials Plus, ISO/IEC 27001, ISO 27017, and ISO 9001 standards, so we can provide customers with robust, consistent assurance in our quality processes and the protection of our systems and customer-related data. We adopt certified frameworks for HMG where data is classified OFFICIAL through to SECRET and above.

What it can do for you

Methods is a GovAssure Independent Assurance Reviewer (Supplier) – experienced and qualified Cyber Security experts providing a GovAssure-CAF Review services to enhance Sector and National Cyber Security Resilience for essential systems and services. Help meet HMG National Cyber Security and associated (company, sector, industry) goals and objectives through adoption of a systematic and comprehensive organisation meets the security requirements associated with GovAssure:

Methods also provide Cyber and Technical services, to support and enable a client to meet the cyber-security standards required of the GovAssure scheme and set-forth by the government, to establish, evaluate and maintain security for UK-CNI.

We are well placed to support and guide an organisation through the complex landscape of cybersecurity, helping develop resilience, guarantee compliance and foster trust in an increasingly digital world. We help our clients to uphold applicable laws and meet statutory requirements, standards and regulations set forth by the government, so that they can establish and sustain security for Critical National Infrastructure (CNI) and systems which underpin CNI across multiple sectors.

Service Features

1. NCSC-assured GovAssure provider delivering high-standard, outcome-focused services
2. NCSC-trained consultants and auditors leading expert, vetted cyber-security teams.
3. Proprietary tooling and templates mapping NCSC CAF across all frameworks
4. UK-wide capability teams supporting rapid deployment
5. NCSC-approved consultancy and service provider for GovAssure, audit, risk management

Service Benefits

1. Professional support and guidance across stages 1-3 & 5
2. Ensures readiness for Stage 4 independent GovAssure review via WebCAF
3. Specialists providing practical recommendations to address risks, vulnerabilities, and controls.
4. Support creation and implementing Stage 5 improvement plan from IAR
5. Assured provider with NCSC certifications and multiple recognised cyber-security standards
6. Supports meeting statutory, legal, industry and sector compliance requirements

Contact details

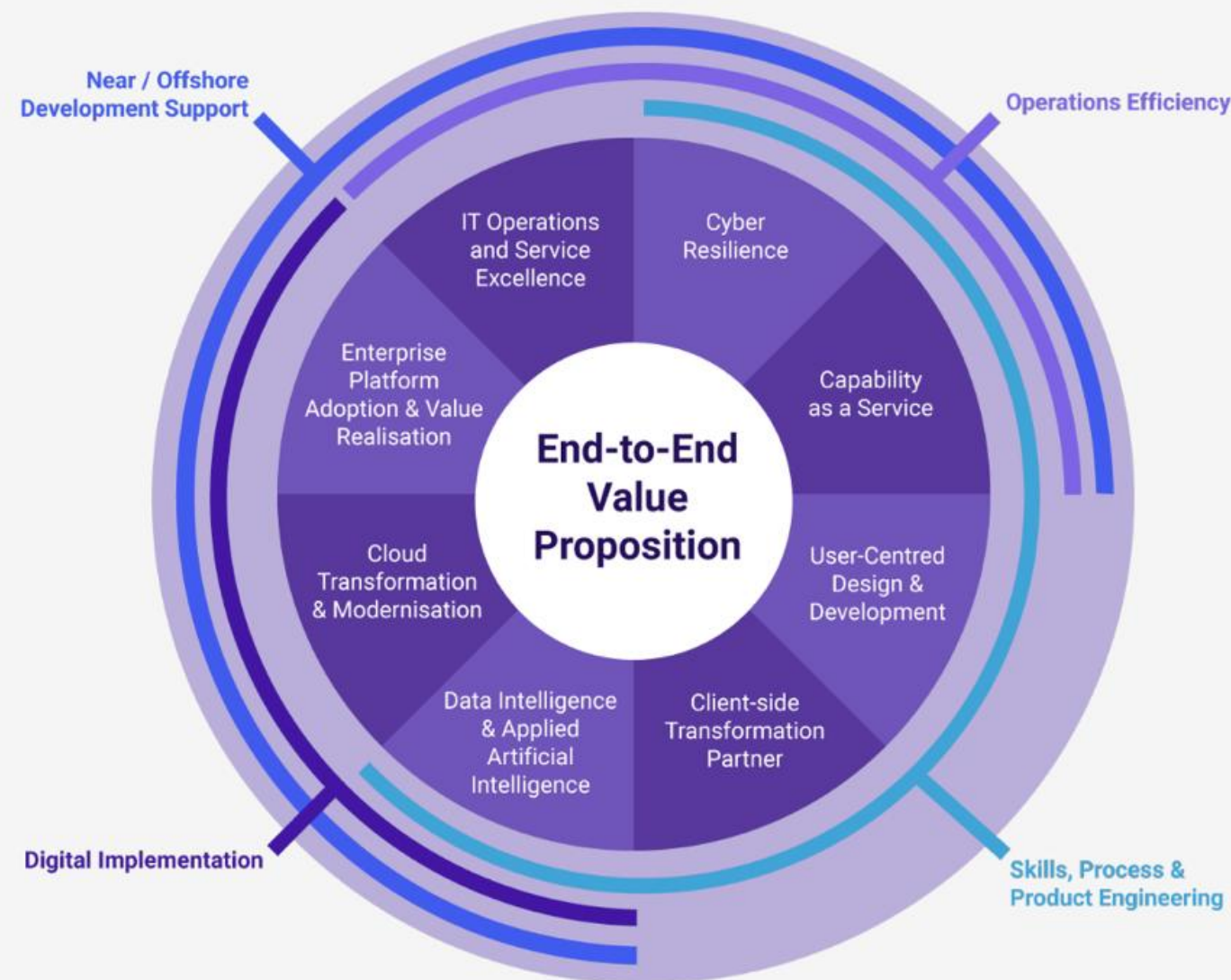
End-to-end transformation and innovation experts

Applying our skills in innovation and collaboration from across the Methods Group, to deliver end-to-end business and technical solutions that are people-centred, safe, and designed for the future.

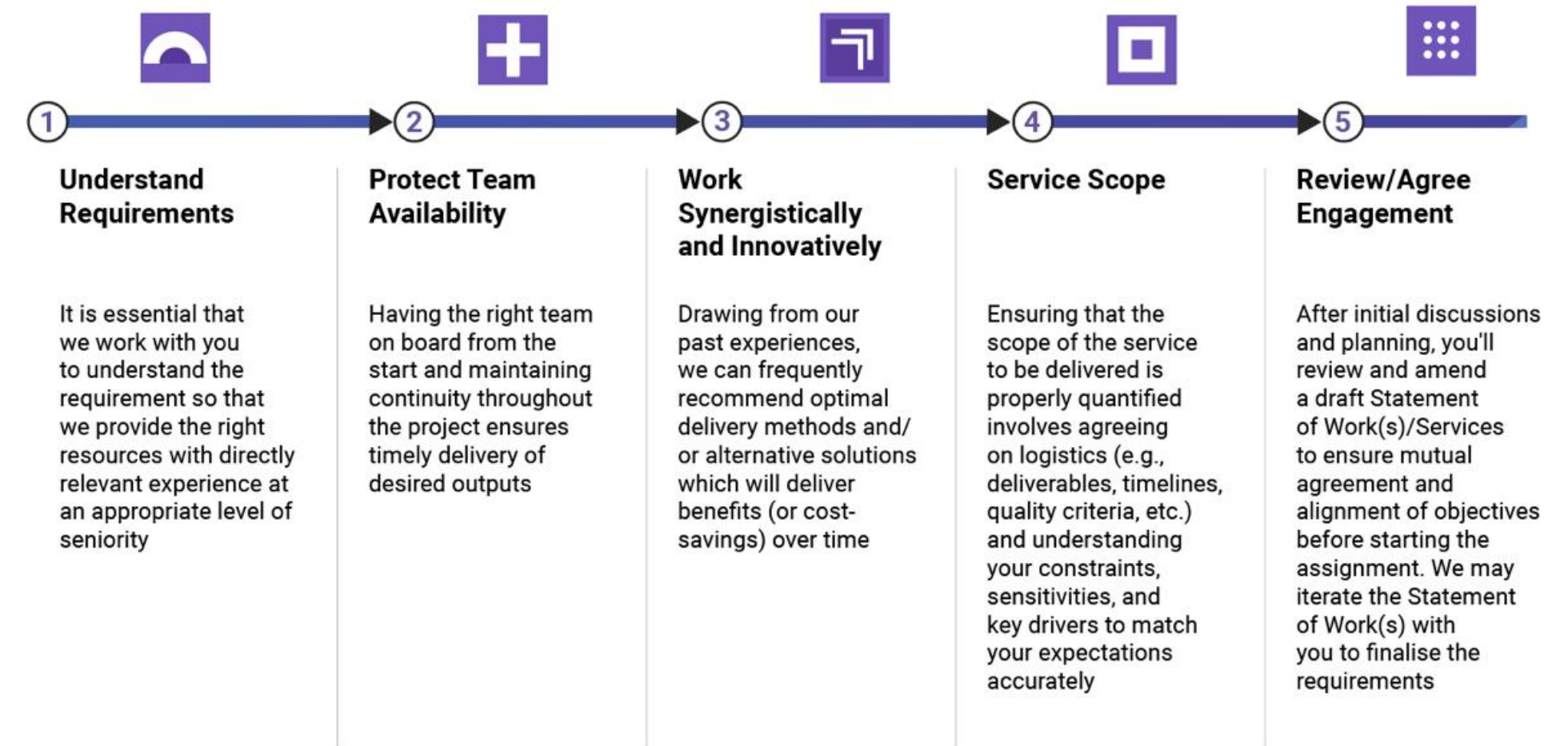
Methods provide collaborative and innovative solutions to help Central Government adapt to the changing landscape and deliver better outcomes for citizens.

With a focus on driving interoperability and innovation in UK Central Government, we have helped multiple organisations in the sector modernise their IT architecture, systems, strategy, and operating models to improve organisational resilience and service delivery.

Methods deliver wide-ranging services and thought leadership to support delivery including:



Onboarding and offboarding process



Ordering and Invoicing

Once we have agreed a Statement of Work(s) we will sign the appropriate agreement and complete a Call Off contract with an attached Statement of Work(s), and submission of a Purchase Order. We will then set up a mutually acceptable start date and commence work.

Payment terms are 30 days or less as may be agreed.

Please note - we are unable to accept Government Procurement Card (GPC) payments.

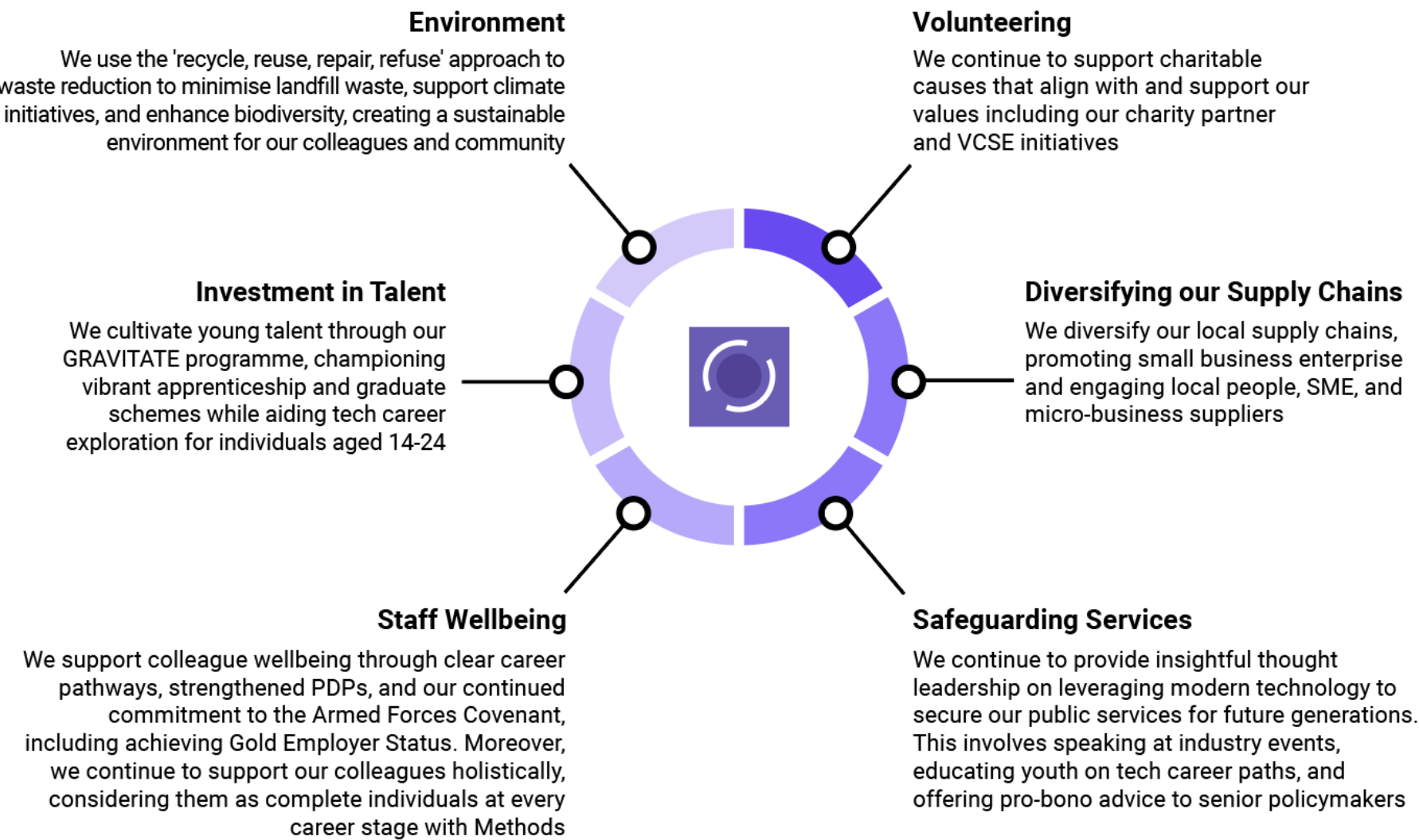


Customer Responsibilities

For any given requirement, we will identify any dependencies on the customer (e.g. access to key stakeholders, facilities, documentation, etc.) and agree these at the start of the work.

Making a difference

The work we do each day is focused on delivering a positive difference for the public sector for the benefit of society as a whole.



Customer stories

Cloud Hosting & Service Modernisation
Modernised digital services using secure cloud hosting, streamlined legacy workflows, and improved data insights. Delivered faster decisions, reduced manual effort, and a more transparent, **user-friendly experience** for internal teams and external users.

Cloud-Based ITSM Consolidation
Unified multiple service desks onto a cloud-based ITSM platform, standardising processes and automating workflows. Improved incident, change, and problem management, **boosting overall service reliability, efficiency, and organisational visibility.**

Large-Scale Cloud Migration (100+ Apps / 120TB)
Delivered cloud migration of **100+ legacy applications** and **120TB of data** with **100% availability**. Strengthened compliance, improved transparency, and significantly enhanced operational resilience across critical digital services.

Azure Migration & Modern Workplace Enablement
Migrated data centres to Azure and deployed modern workplace cloud services, delivering secure, scalable infrastructure. Achieved improved user experience, strengthened security posture, and **£1m savings** - all with zero service disruption.

Cloud ITSM Migration (ServiceNow SaaS)
Successfully migrated from a legacy ITSM tool to a modern, cloud-based ServiceNow platform. Delivered scalable, robust service operations, strengthened governance, and enabled faster, more consistent digital service delivery across the organisation.

Cloud-Native Data Pipelines (Azure Integration)
Built automated Azure Data Factory pipelines into a Lakehouse architecture, using Bronze/Silver/Gold layers and Delta with CI/CD. Delivered secure daily refreshes, improved data quality, lower manual effort, and more efficient reporting.