

G-Cloud 15 Service Description

AI Governance & ISO 42001 Assessment

Artificial Intelligence Management

Methods’ AI Management Service allows organisations to develop and deploy trustworthy, resilient, and secure AI solutions aligned with industry best standards. With NCSC assured experts alongside AI Governance Professionals, our teams work with organisations to ensure their AI is fit for purpose and ensuring Confidentiality, Integrity, and Availability of data.

What is the Service

Methods is an NCSC Assured Cyber Consultancy, demonstrating a proven track record of delivering cyber security consultancy expertise undertaken by suitably qualified and experienced personal as defined by NCSC and the UK Cyber Security Council.

As an NCSC Certified Consultancy our consultancy services are scoped, planned and delivered in line with ISO 20700, the delivery of Management Consultancy services. This requires us to engage and work closely with our clients to ensure that the services we provide have been aligned with industry best standards.

We are a leading provider of Artificial Intelligence (AI) services across government, with a proven track record of delivering successful projects for clients across various sectors and regions. Therefore, we understand the challenges with AI governance, and we can leverage this experience to help design, implement, and manage an AI Management System (AIMS) in line with ISO 42001 and NIST AI RMF requirements, that suits your specific needs and goals, using the best-in-class tools and technologies. We can also provide you with ongoing support and guidance, ensuring that your AIMS is always up to date and effective.

Our experts are certified AI Governance Professionals (AIGP), showcasing knowledge and skills in AI Laws and Standards, AI development Life Cycle, Risk Management and many more domains. We have experience of conducting analysis against industry best practice to:

- Provide independent risk- and compliance-based audit assessments
- Support compliance with HMG security objectives, policies, and standards
- Integrate with NCSC National Cyber Security Strategy
- Aid in the production of policies.

Compliance with relevant regulations and standards including but not limited to:

- NIS regulations and ISO 27001
- NCSC Cyber Assessment Framework (CAF)
- Sector specific compliance requirements
- GovAssure.

We provide a systematic and measurable technical assessment of policies and practices that will enable the organisations AI management system. Which in turn, enables an iterative procedure of determining and maintaining the output of the deployed AI.

The scope of our service will be tailored in collaboration with the organisations to ensure alignment to business unit or strategic roadmaps. We collaborate with key stakeholders in the planning phase to ensure stakeholder engagement throughout the project lifecycle. It’s vital that management are engaged as this will enable effectiveness in establishing good practice and identification of areas of continuous improvement.

We adopt an Agile methodology, designed to integrate seamlessly into the organisation, complementing and innovating current working practices.

We recognise that an effective AI management service enables an organisation to ascertain vulnerabilities, weaknesses in existing processes and procedures, control gaps and weaknesses across your current AI deployment. Our capability can provide insight and support improvements across:

- Risk Management
- Security Governance
- Ensuring trust within the AI system
- Legal and regulatory compliance requirements
- Business Continuity
- Incident Management
- Security Training and Awareness
- Data Security

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 collaboratively 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.

Methods resources 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. Methods has a large pool of SC and DV cleared UK personnel and has experience of designing, building, and maintaining governance and security to deliver service offerings at OFFICIAL, SECRET and ABOVE SECRET classifications.

Contact details

What it can do for you

An AIMS allows organisations to deploy AI assets with the knowledge they are governed and managed effectively. ISO 42001 sets forth guidelines for the governance of AI throughout its lifecycle, encompassing aspects such as planning, development, deployment, operation, monitoring, and continuous improvement. This section delves into the principles and processes outlined in ISO 42001, emphasising its focus on risk management, ethics, transparency, accountability, and stakeholder involvement.

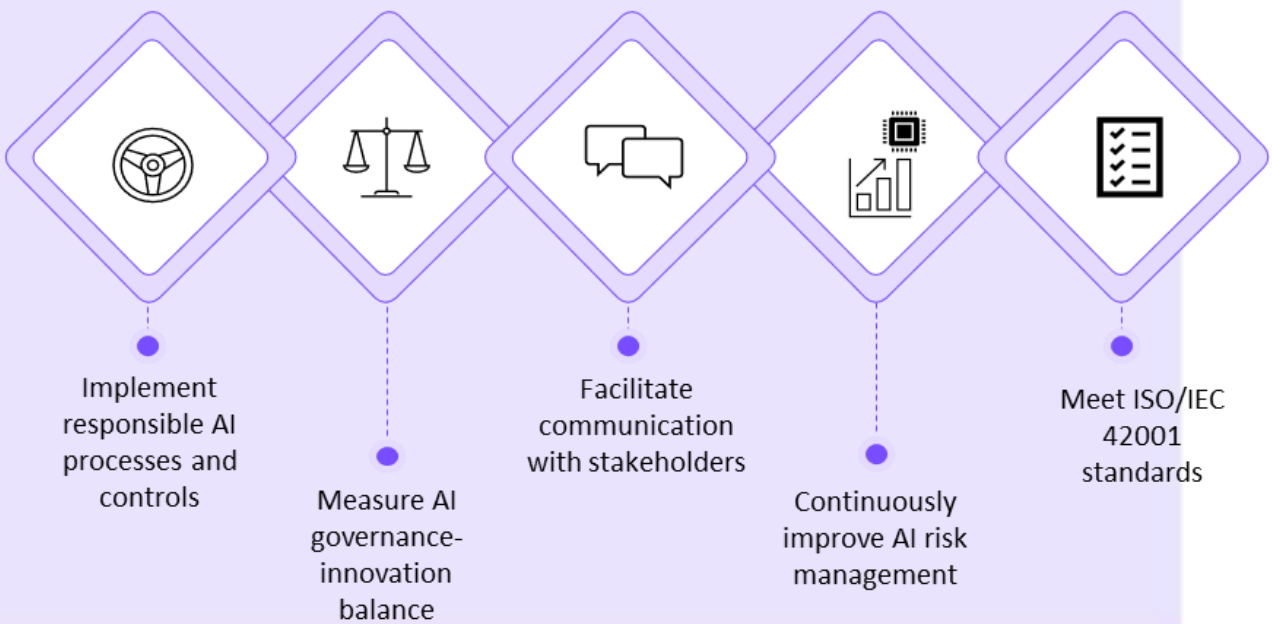
NIST AI RMF provides a structured approach to managing risks associated with AI systems, drawing upon established risk management principles adapted to the unique characteristics of AI technologies. This section examines the core elements of NIST AI RMF, including risk assessment, mitigation strategies, validation, and ongoing monitoring, highlighting its alignment with established cybersecurity frameworks.

By utilising both ISO 42001 and NIST AI RMF frameworks Methods are able to create robust AI Management Systems allowing organisations to deploy effective, trustworthy, secure and accountable AI assets in their organisation.

AI Management Systems offers several business benefits, such as:

- Comprehensive Lifecycle Approach: ISO 42001 offers a holistic framework that covers the entire lifecycle of AI systems, including planning, development, deployment, operation, monitoring, and continuous improvement.
- Transparency: ISO 42001 promotes transparency and accountability in AI governance by requiring organisations to document and communicate their AI-related policies, procedures, and decisions.
- Risk Focused: By being risk focused we can use risk-based approach to ensure risks are identified assessed and mitigated allowing organisations to make informed decisions about risk tolerance and risk treatment strategies.
- Flexibility: Both ISO 42001 & NIST are designed to be flexible and scalable allowing organisations to tailor their risk management approach to their AI needs.
- Stakeholder Involvement: By engaging stakeholders, we can ensure that the AI system incorporated is fit for purpose and address stakeholder needs.
- Policy: At Methods we can help organisations create tailored policy for the governance and management of AI.
- Certified AI Governance Professionals (AIGP): Our experts are certified experts in AI Law & Standards, AI Development Lifecycle, AI Risk Management.

ISO 42001 Benefits



Service Features

1. Create policy for ethical, accountable & trustworthy AI systems
2. Conduct AI risk assessments & create mitigation strategies
3. Formulate robust policies aligned with ISO42001 standards for implementation
4. Design, deploy tailored controls to protect systems aligned with ISO42001
5. Develop detailed plans to address and mitigate security incidents effectively
6. Conduct sessions to educate/raise awareness on security practices around AI
7. Establish mechanisms for ongoing monitoring, evaluation, and ISMS improvement
8. Provide a system aligning with ISO 42001 requirements
9. Provide a framework for the responsible development of AI systems
10. Create a Risk-Based approach for Artificial Intelligence management

Service Benefits

1. Establish a resilient framework for your and AI Management System
2. Attain industry best practices, leading to ISO42001 alignment
3. Enhance customer satisfaction and competitive positioning with AI implementation
4. Improve the reliability and effectiveness of numerous services
5. Offer an agreed, repeatable method for managing the implemented framework
6. Safeguard company Information in terms of confidentiality, integrity, and availability
7. Ensure the presence of people/processes/policy to protect AI assets
8. Provide a risk-based approach to maintaining your AIMS
9. Consolidate the experience and expertise of all involved parties

Contact details

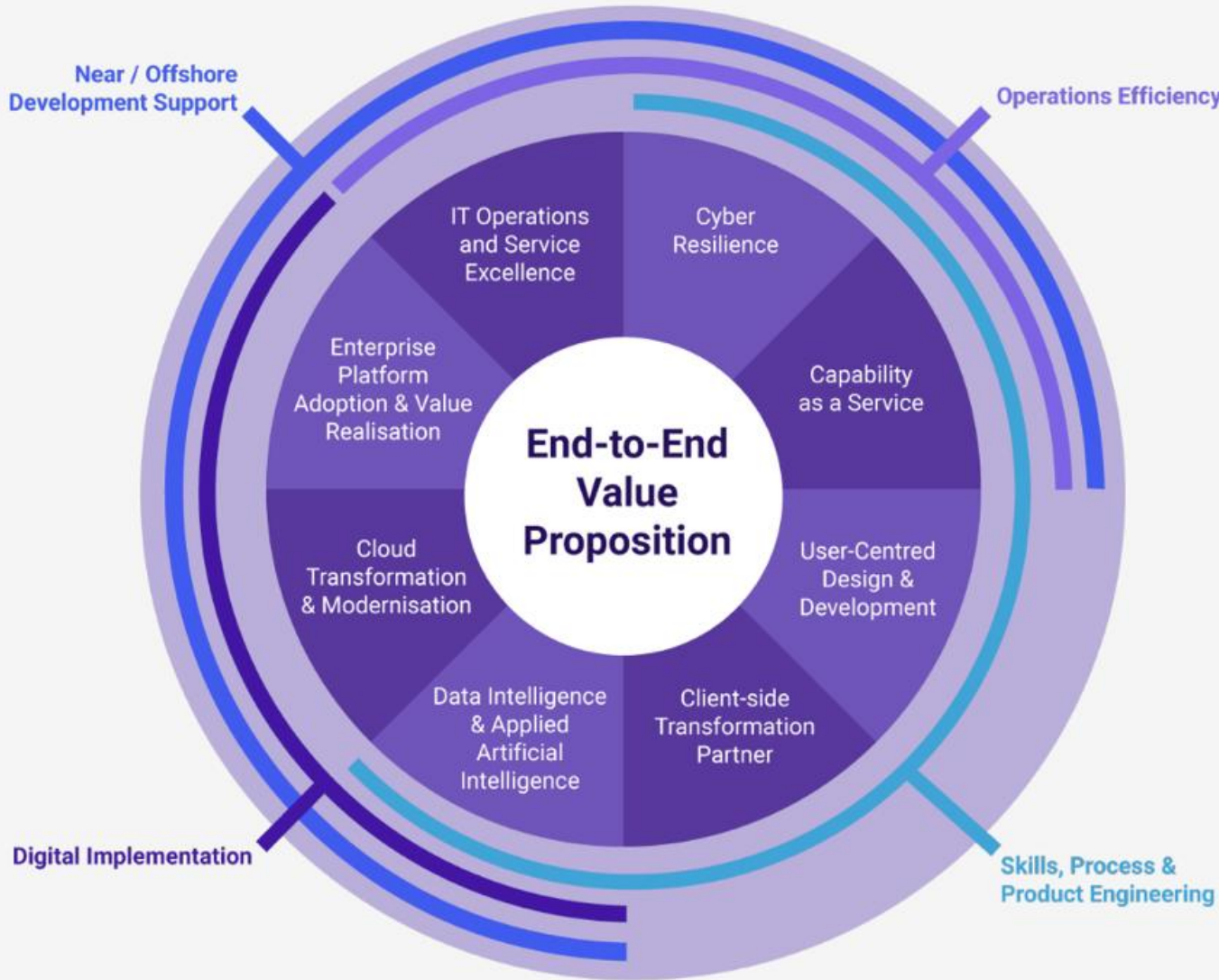
End-to-end transformation and innovation experts

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.

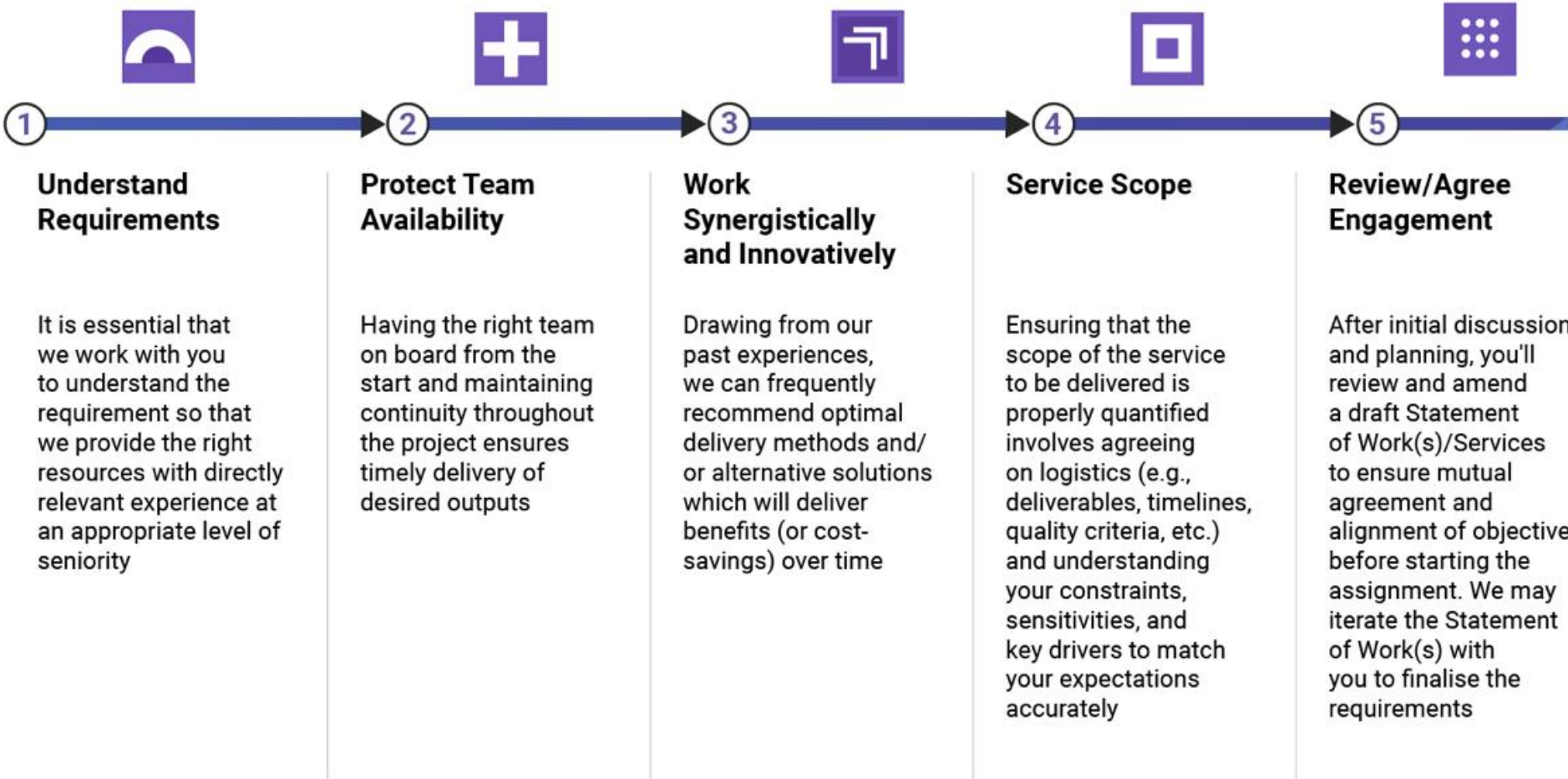
Methods provide collaborative and innovative solutions to help Central Government adapt to the changing landscape and deliver better outcomes for citizens.

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.

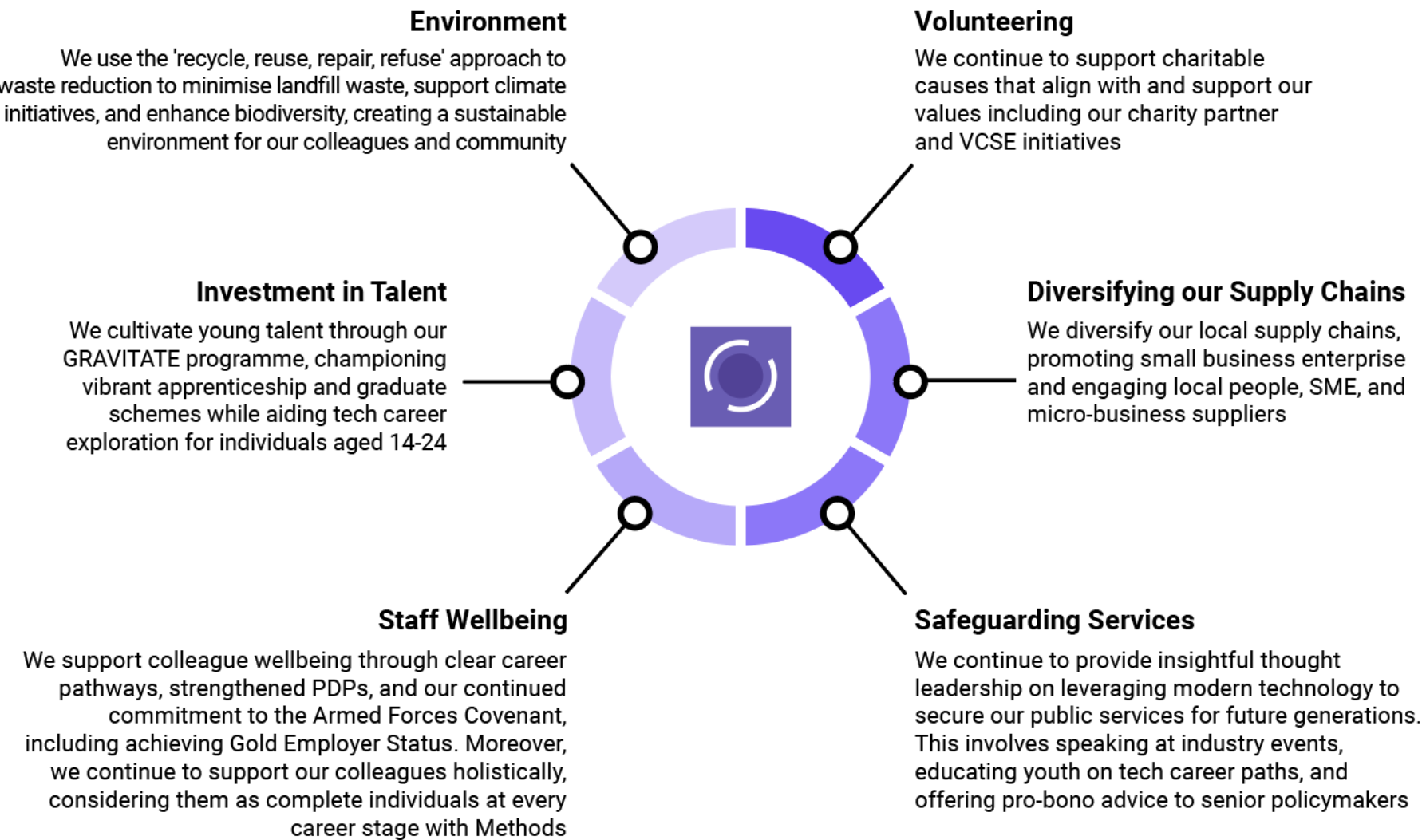


Customer Responsibilities

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.

