Capgemini

Climate Risk and Resilience
G-Cloud 15

Table of Contents

1 Service Overview 3
2 Business Need 3
3 Our Approach 4
4 Buyer Responsibilities 6
5 Service Management 6
6 Protection of Data 6
7 On-boarding and Off-boarding 6
8 Skills and Knowledge Transfer 6
9 Vendor Accreditations/Awards 6
10 Sub-contractors 7
11 Business Continuity and Disaster Recovery 8
12 Pricing 8
13 Ordering and Invoicing 8
14 Termination Terms 8
15 Further Information 8

1 Service Overview

This offer enables the UK Public Sector to address climate risks impacting their digital and technology infrastructure and cloud services by embedding climate resilience and adaptation into departmental strategies, priorities, and aligning with key regulatory frameworks (such as Greening Government Commitments, 3rd National Adaptation Programme, Cyber Security and Resilience Bill, others). This offer provides government services with an end-to-end view of the impacts of a range of climate risk hazards on information technology and digital infrastructure and associated operations, supply chains, and value chains, providing key climate risk hotspots and resilience requirements to be addressed.

Making use of Capgemini's climate risk tooling, domain expertise, and partner ecosystem, this offer enables government services to gain tailored climate risk assessments based on specific problem statements and hypotheses and highlights appropriate climate mitigation, management, and adaptation options to ensure IT and digital hardware and software are resilient and adaptive to climate risks and enable continued service of cloud services and critical functions. This offer, additionally, helps government services address and embed topics of climate risk, climate change mitigation, and climate change resilience and adaptation at cross-sector, organisational, supply chain, and value chain levels by helping government services develop digital resilience and adaptation strategies, and associated operating and governance models.

2 Business Need

The climate crisis is no longer a future concern; it is an on-going reality disrupting business value chains on a global scale. Between 2000 and 2024, climate-linked disasters have caused over $3.6 trillion in economic damage, with storms accounting for 60%, floods 27%, and droughts 7%. By 2050, climate change is expected to cause damages to agriculture, infrastructure, productivity, and health estimated at $38 trillion per year.

The UK's Public Sector will be especially impacted by these physical climate risks, with many government services already experiencing disruptions and loss to assets and productivity, availability of raw materials, and biodiversity and natural resources, particularly due to extreme weather events and their systemic impacts. Disruptions to the Information and Communications Technology (ICT) sector, particularly as the reliance on digital and cloud services increases, will exacerbate the disruptions and losses government services will experience due to climate risks. In the UK, heatwaves and water stress have been identified as the highest climate risks for critical national infrastructure (CNI) such as data centres, with 45% of data centres having experienced an extreme weather event. The World Economic Forum estimates such climate risks could increase annual cumulative data centre running costs by $3.3 trillion. Furthermore, the rise in AI adoption and high-performance computing (HPC) will add complexity, with increased use of high-performance computing for AI leading to increased demand for electricity and cooling to maintain ambient temperatures will make data centres more vulnerable to climate events. Disruptions to the digital backbone of the Public Sector can trigger cascading failures across core functions such as health care provision, financial stability, energy security, and national security. Failure to navigate these systemic, cascading risks could negatively impact capital and operational expenditure requirements across government services, increase operational disruptions and threaten service continuity, decrease data veracity, and increase exposure to cyber-exploitation and threats.

Climate resilience and adaptation is a strategic imperative for the UK Public Services, as evidenced by frameworks such as The Climate Change Act 2008, National Adaptation Programme, Greening Government Commitments, and many more. Climate adaptation is the set of proactive measures undertaken by an organisation to prepare for, and adjust to, the current and future impacts of climate change across their value chains. For government services, long-term sustainability, operational continuity, and security will depend not only on decarbonisation, but also on embedding resilience and adaptation across value chains. As per the LSE Grantham Institute, failure to integrate proactive climate resilience and adaptation measures could cause damages equivalent to 3.3% of the UK's gross domestic product (GDP) by 2050 and at least 7.5% by 2100. Embracing climate resilience and adaptation across government services will be imperative for the UK Public Sector to ensure operational continuity and long-term security – resilience and adaptive digital and technology infrastructure is a critical component of this.

As of 2026, digital and technology infrastructure resilience is a foundational requirement for the UK Government (as evidenced by frameworks such as Cyber Security and Resilience Bill, 3rd National Adaptation Programme). As government services accelerate their digital transformation, the risk of climate inaction (and not considering climate impacts in this transformation) grow significantly. Embedding climate resilience and adaptation into digital and technology infrastructure and cloud services will be critical to safeguard the delivery of public services. To address these systemic challenges, our approach provides a comprehensive, end-to-end framework for embedding climate risk, resilience, and adaptation across the UK Government's digital and technology estate.

3 Our Approach

Digital and technology infrastructure is the backbone of modern public services. As climate risks escalate and the rapid adoption of AI and high-performance computing further increases pressures on energy, cooling, and water requirements, digital and technology infrastructure will become more susceptible to cascading vulnerabilities. These vulnerabilities may range from heat and water stress driven disruptions to service and operational continuity across critical national infrastructure (such as data centres) to increased risk of cyber-exploitation and cybersecurity breaches. Climate-driven impacts to digital and technology infrastructure will have significant impacts on government services, especially associated with delivery of safe and effective health care, maintaining financial stability, and effectively protecting national security.

Our approach enables government services to address and manage these systemic risks with an end-to-end climate risk, resilience, and adaptation framework, tailored to the specific priorities, maturity, and requirements of government services.

Our climate risk, resilience, and adaptation framework comprises of three domains – Commit, Act, and Monitor & Report structure, enabling government services to:

1. *Commit* to embedding climate risk, resilience, and adaptation into strategy and business models by focusing on identifying climate change-linked strategic, operational, financial, and market risks, developing tangible action resilience and adaptation plans, and develop the appropriate culture across workforce and suppliers to enable the action plans.
2. *Act* to integrate climate resilience and adaptation across functions, supply chains, and value chains through the development of innovative products and services, building resilience across supply chains and operations, and climate-proofing digital and IT infrastructure and associated assets.
3. *Monitor and Report* to enable the monitoring and evaluation of resilience and adaptation actions, ensure data veracity, and enable alignment and reporting against critical frameworks and regulations.

Commit – Climate Risk, Resilience, and Adaptation Strategy and New Business Models:

The first domain of the framework establishes the foundational strategy and governance processes required to identify, assess, and embed climate resilience and adaptation into core organisational functions and supply chains.

1. **Climate Risk Modelling and Impact Assessment:** undertake climate risk modelling and impact assessments to identify and assess physical and climate risks material to digital and technology infrastructure within government services across climate scenarios and time horizons. Create a baseline and maturity analysis for climate risk, resilience, and adaptation, aligning the analysis with the relevant regulatory landscape and compliance requirements. In doing so, we enable government services to identify and quantify their climate risk exposure across a wider range of climate hazards and develop a baseline understanding of current and desired climate maturity, enabling data-driven decision-making, targeted resource allocation, and complete regulatory compliance with standards such as Greening Government Commitments, Government Buying Standards, Digital Procurement Framework, and many more.
2. **Resilience and Adaptation Planning, Strategy, and Policy Set Up:** define the vision, strategies and action plans to address climate risks and levels of exposure identified, setting a clear strategic direction and exploring new business models to embed resilience and adaptation into operations, supply chains, products, and services. Align organisational policies, processes, and governance mechanisms with resilience and adaptation goals and actions to drive successful delivery of the actions and positive impact. Embedding resilience and adaptation into organisational strategy, processes, and governance mechanisms enables defining a clear strategic direction and fosters innovative.
3. **Upskilling for Climate Resilience and Adaptation:** develop and action upskilling plans aligned with resilience and adaptation strategies, organisational priorities and functions, and regulatory landscape to build capacity improve the climate maturity of the workforce, suppliers, and partner ecosystem, ensure the successful deliver of resilience and adaptation plans, and reduce supply chain risks.

Act – Climate Resilience and Adaptive Value Chains:

The second domain of the framework translates strategy into action, ensuring operations, supply chains and core products and/or service offerings are resilient to climate risks.

1. **Climate Resilient and Adaptive Value Chains:** identify existing and/or design new products and services that will help achieve resilience and adaptation goals, embedding resilience and adaptation into design cycles and aligning products. Leverage the products and services to understand future climate risk requirements and public needs for resilience and adaptation to further iterate products and services.
2. **Climate resilient and adaptive operations and supply chains:** identify end-t-end supply chain and operational strategies to manage, mitigate, and/or adapt to the cascading impacts of climate risks and the associated digital and technological failures they may trigger. Align adaptation strategies with organisational priorities, workforce requirements, and supplier needs to facilitate cross-departmental collaboration and public-private partnerships to improve resilience across critical national infrastructure that digital services rely on.

Monitor & Report – Data for Climate Resilience and Adaptation:

The third domain of the framework prioritises data to monitor and evaluate climate performance across government services, enabling transparency and alignment of resilience and adaptation efforts with key compliance requirements.

1. **Monitoring, Reporting, and Compliance:** assess resilience and adaptation actions against regulatory and compliance requirements, key internal and external priorities, defined metrics, and key performance indicators to track progress, build transparency, and establish regulatory confidence. Leverage key assets, such as the Adaptation Data Hub, to track the performance of resilience and adaptation actions, perform audits and due diligence, and establish the required course corrections to ensure the success of resilience and adaptation actions.
2. **Communications:** Build stakeholder specific communications for climate risk, resilience, and adaptation to share best practices, key outcomes, and benefits (environmental, social, and financial) to enable internal government-wide buy-in and external supplier and partner ecosystem action and establish trust with the public.

Our approach allows government services to holistically address the systemic, cascading impacts of climate change, enabling them to strive towards a more resilient digital future.

Our approach enables clients to address end-to-end climate risk, resilience, and adaptation of digital and technology infrastructure through a combination of services based on clients' maturity, priorities, and requirements:

4 Buyer Responsibilities

Please refer to the Supplier Terms listed with this service on the Platform. These may contain additional Buyer obligations/costs the Buyer is subject to that are not identified anywhere else in the Supplier's Application or on the Platform.

5 Service Management

Does not apply to this offer.

6 Protection of Data

This service is based on a security classification of 'Official', however should you have a requirement for a different security classification that you would like us to consider, please contact us to discuss.

7 On-boarding and Off-boarding

Capgemini shall undertake on-boarding and off-boarding activities agreed within the Order Form (including as a minimum an exit plan in line with the Call-Off Contract terms) which will be charged for in accordance with the Pricing section for this service.

8 Skills and Knowledge Transfer

Capgemini recognises that skills and knowledge transfer is a critical element in the provision of G-Cloud services to public sector clients. Where possible and applicable, this forms part of the delivery plan for the service agreed at the start of the engagement. Our consultants and engineers are experienced in providing skills and knowledge transfer for major private and public sector clients.

Where appropriate, we may use a standard approach, tailored to topic, skills-gap and individual, to facilitate consistency and effectiveness. The approach, Capgemini's Assess-Plan-Implement framework, has been used repeatedly by our teams to structure the work involved in transferring skills and creating new teams capable of driving and sustaining change long after the end of the formal programme. The framework can be applied throughout a project to understand knowledge transfer objectives, plan training delivery methods and materials, and deliver and evaluate success.

9 Vendor Accreditations/Awards

For the 13th year in a row, Capgemini has been recognised as one of the World's Most Ethical Companies® by the Ethisphere® Institute. This is an acknowledgement of our ethical culture that makes us an employer of choice and responsible player in the eyes of our clients, shareholders, and the wider community.

ISO 9001 Quality Management for Management Consultancy and IT Implementation and services to the Public Sector

ISO 27001:2013 - Provision (Delivery) of IT services including business applications development, maintenance and Data, Digital and Cloud technologies.

NelsonHall has identified Capgemini as a Leader in its 2022 NEAT Vendor Evaluation for Learning Services due to its ability to meet future client requirements as well as its capability to deliver immediate learning benefits to them.

Capgemini is the first amongst consultancy and technology firms to be recognized six times in a row for its thought leadership reports.

2023 Ecovadis Platinum Rating: We maintained a platinum rating, recognising us as a responsible and sustainable business in the top 1% of companies assessed.

Better Society Awards: Our collaboration with Code Your Future to offer digital skills training won a Better Society Award in 2022. The awards celebrate efforts by commercial organisations to create a better society.

Inclusive Top 50 UK Employers List: We achieved second place in the Inclusive Top 50 UK Employers List 2022/23 – a list that assesses companies for best practice on diversity, equality and inclusion

UK Best Workplaces for Women: We were listed as a Best Workplace for Women by Great Place to Work®. This listing is based on responses from our team to an anonymous survey about their employee experience.

UK Best Workplaces for Wellbeing: We are listed by Great Place to Work® as a Best Workplace for Wellbeing

Great Place to Work: We were certified as a Great Place to Work® in 2023, reflecting our employees' experience of working at Capgemini in the UK.

10 Sub-contractors

Capgemini UK may use the following subcontractors to deliver this service:

- Capgemini Technology Services India Limited.
- Capgemini France

11 Business Continuity and Disaster Recovery

No disaster recovery plan is provided as part of these Services.

12 Pricing

This service is priced in accordance with the SFIA Rate Card attached. Capgemini can also provide offshore resources at reduced rates where appropriate. Projects can be priced either on a Time & Materials or Fixed Price basis.

13 Ordering and Invoicing

Please refer to the Supplier Terms for this service.

We would be pleased to arrange a call or meeting to discuss your requirements of our service in more detail.

14 Termination Terms

Please refer to the Supplier Terms for this service.

15 Further Information

For more information about this or any of our G-Cloud services, please contact our Public Sector Team.

Phone: 0370 904 4858

Email: publicsector.opps.uk@capgemini.com including the following information:

1. The name of this service.
2. The name of your organisation.
3. Your name and contact details.
4. A brief description of your business situation.
5. Your preferred timescales for starting the work.

About Capgemini

Capgemini is a global business and technology transformation partner, helping organizations to accelerate their dual transition to a digital and sustainable world, while creating tangible impact for enterprises and society. It is a responsible and diverse group of 340,000 team members in more than 50 countries. With its strong over 55-year heritage, Capgemini is trusted by its clients to unlock the value of technology to address the entire breadth of their business needs. It delivers end-to-end services and solutions leveraging strengths from strategy and design to engineering, all fueled by its market leading capabilities in AI, generative AI, cloud and data, combined with its deep industry expertise and partner ecosystem. The Group reported 2024 global revenues of €22.1 billion.

Make it real. | www.capgemini.com