(Cloud)
Engineering
Advisory
Security

GCloud 14 Cloud Support
Service Descriptions
V1.0 May24
Cloud-Dog Solutions

d

Mission Statement

Deliver IT enabled Change, in Automation, Agility, Strategic Planning and cloud delivery. Make the changes needed to improve your security posture. Reach internationally recognised levels of quality (GDPR, ISO27k, ISO20000) to meet your compliance obligations. Integrate your Service Operations, Security and Compliance, to enable quality delivery.

Cloud Security Design

Cloud Security Design

Service Description

Enhance cloud security with our comprehensive Cloud Security Design service. Specialising in defining security requirements, designing robust architectures, and implementing critical controls like firewalls and encryption. Our service includes continuous vulnerability assessments, security monitoring, and incident management to ensure confidentiality, integrity, and compliance while effectively managing risks and costs.

Features

- Develop policies, guidelines, standards tailored to your cloud risk appetite.
- Deploy technical/administrative controls for ISO27001 and Cyber Essentials compliance.
- Integrate cybersecurity within the agile software development lifecycle/GDS approach
- Identify/mitigate risks identified with Technology Codes of Practice.
- Ensure your cloud solutions meet DPA and cyber protection standards.
- Embed security skills within projects across the delivery lifecycle
- Architect encryption/network controls to protect data in-transit/at-rest.
- Automation to enhance compliance platform, boundary and network controls.
- Operationalise continuous monitoring and incident response to maintain security.
- Design the Security Architecture to ensure mitigation for multi-cloud services.

Benefits

- Enhance internal security capabilities and compliance understanding.
- Reduce cybersecurity risks through proactive control implementation.
- Accelerate regulatory compliance across cloud environments.
- Strengthen data protection with advanced security measures.
- Enable security to seamlessly integrate into software development cycles.
- Boost operational efficiency with automated security solutions.
- Improve risk management with detailed assessments and strategies.
- Facilitate swift compliance with evolving technological standards.
- Empower teams with expert resources and security skills.
- Design cloud architecture for safer, faster service delivery.

Overview

Our Cloud Security Design service offers a comprehensive approach to securing cloud architectures. Specialising in the creation of security policies and the implementation of essential controls, our service ensures controls and defence mechanisms are in place for firewalls, encryption, and compliance, aligned with standards such as ISO27001, NIST and Cyber Essentials. From continuous vulnerability assessments to proactive incident management, we provide full-spectrum security oversight to maintain confidentiality, integrity, and compliance across your cloud operations. This service is ideal for projects that require stringent security measures integrated within the agile development lifecycle, aiming to enhance internal capabilities, reduce cyber risks, and streamline compliance processes in cloud environments. We equip projects with expert resources and skills necessary for secure, efficient, and compliant cloud service delivery.

Service Features

Our "Cloud Platform Design" service helps provide structure and enhanced protection to cloud environments against emerging threats, and deliver compliance with regulatory standards. Some of the key features that define our comprehensive service offering:

- **Security Policy Development**: We craft tailored security policies, guidelines, and standards that align with your organisation's specific cloud risk appetite. This foundational work ensures that all subsequent security measures are cohesive and robust, providing a structured approach to managing cloud risks.
- **Comprehensive Controls Implementation:** Our service includes the deployment of both technical and administrative controls to meet the stringent requirements of ISO27001, CIS, NIST and Cyber Essentials. This approach helps ensure that operational practices contribute to overall security posture.
- **Agile Integration**: Recognizing the dynamic nature of cloud development, we integrate cybersecurity measures within the agile software development lifecycle. This integration ensures that security is a continuous consideration throughout the project, from initial design through deployment, adhering to the Government Digital Service (GDS) approach.
- **Risk Management**: Leveraging Technology Codes of Practice, this service will help identify and mitigate potential security risks. Using a proactive risk management strategy, the service can deliver detailed assessments to drive implementation, and hence prevent security breaches.
- **Data Protection Standards Compliance**: Ensuring compliance with DPA/GDPR and other standards is paramount. Our Service will assist in incorporating encryption and network controls to safeguard data both in-transit and at-rest, thus upholding the integrity and confidentiality of sensitive information.
- **Security Architecture for Multi-Cloud Environments**: We architect comprehensive security solutions that are scalable across multi-cloud environments. This capability ensures that security measures are not just confined to a single supplier/cloud platform but are extensive and adaptive to various cloud services used by the organisation.
- **Automation of Security Processes**: By automating compliance and security processes (Compliance as Code, Infrastructure as Code), we can help enhance the efficiency and accuracy of boundary and network controls. Automation aids in maintaining consistent security standards across all cloud operations and reduces the possibility of human error.
- **Continuous Monitoring and Incident Response**: Operational security design to provide continuous monitoring and agile incident response. This ongoing vigilance allows for the immediate detection of and response to security incidents, minimising potential damages and disruptions.
- **Skill Embedment and Empowerment**: Expert resources that can empower your internal teams with the necessary security skills. Fosters a culture of security awareness and competence within your organisation, enhancing the overall security resilience.

Key Outcomes

Our Cloud Security Design service delivers key outcomes for organisations that can significantly enhance the security posture, reduce risks and compliance of your digital programmes.

- **Improved Compliance:** Adherence to international and industry-specific compliance standards. Our service ensures that your cloud infrastructure complies with DPA, ISO27001, Cyber Essentials, and other relevant regulations. This comprehensive compliance support helps mitigate legal and operational risks associated with non-compliance.
- **Reduced Security Risks:** By implementing technical and administrative controls, with automated risk assessments, our service can help minimise the vulnerabilities of your cloud solutions. Our proactive approach to identifying and mitigating risks ensures that potential threats are addressed before they can impact your operations, significantly reducing your overall security risk profile.
- **Enhanced Assurance and Confidence:** Using the recognised frameworks and continuous monitoring tooling, we can help you gain increased assurance and confidence in the cloud security posture. This oversight ensures that security measures are functioning optimally and that any deviations are quickly rectified, providing peace of mind and reliability in security execution.
- **Demonstrated Alignment to Standards:** Provide feedback that the implementations of controls are in line with cyber standards and best practices. This helps to demonstrate to stakeholders and regulators that your service upholds the right security measures.
- **Security Integration in Development:** Integrate security practices into the agile software development lifecycle, ensuring that security design and controls are embedded from the outset. This integration helps reduce the need for costly and disruptive adjustments post-deployment.
- **Architecting Secure Cloud Infrastructures:** Our service designs secure, scalable cloud platforms capable of meeting the specific challenges of your services. By bridging agile development practices with rigorous security requirements, we create environments that support both dynamic development needs and stringent security demands, ensuring that your digital solution is both versatile and robust.

How our Service can help you.

Our service can help you enhance digital programme and service delivery crucially by enhancing design, development and operations, across platform engineering and project delivery. By integrating this service, senior stakeholder can expect the following advantages:

- **Enhanced Security Outcomes Reduce Cyber Risks**: Establish security processes from the outset, significantly reducing potential vulnerabilities. Our proactive approach involves identifying and mitigating risks early in the project lifecycle, which not only secures operations but also prevents costly disruptions and data breaches. This systematic risk management approach boosts the overall security posture of your cloud environments.
- **Integrated Security Practices**: By embedding security measures and considerations into the design and development lifecycle, our service ensures that security is a cornerstone of both solution and platform development and not an afterthought. This helps streamline the development process, and reduce the iteration cycles often required to retrofit security into developed systems; saving time and reducing costs.
- **Expertise and Skill Provision**: Bring top-tier skills and extensive experience in cloud security to your projects, ensuring that best practices in cybersecurity are adhered to throughout your project’s development and operational phases. This support spans the full service lifecycle, enhancing both the strategic and tactical aspects of project execution.
- **Stakeholder Confidence**: Providing transparent, consistent, and verifiable security measures helps to instil confidence among business and external stakeholders. Through demonstrating compliance with industry standards like GDPR, ISO27001, and NIST, this service assures stakeholders of the commitment of the programme to secure and handling responsibly personal and confidential information.

- **Operational Efficiency and Compliance**: Aid the achievement and maintenance of meeting compliance across standards, ensuring that security implementation is up to date and effective. Compliance not only protects the organisation from potential legal and reputational consequences but also improves operational efficiency, allowing teams to focus on innovation and core business goals without being hindered by compliance issues.

Supported Roles

The following roles help deliver the Cloud Security Design process, and are aligned to this service offering.

- **Security Architect (SFIA: Information Security, GDS: Security Architect):** Designs secure cloud architectures and develops policies for cloud security. This role ensures that all designs adhere to best security practices and compliance standards.
- **Security Engineer (SFIA: Systems Installation/Decommissioning, GDS: Security Engineer)**: Implements and maintains the security measures necessary to protect cloud services. This includes setting up firewalls, intrusion detection systems, and encryption protocols to secure data transactions.
- **Compliance Manager (SFIA: Quality and Compliance Management, GDS: Service Manager):** Oversees compliance with ITIL, DPA, ISO27001, and other regulatory frameworks. Manages audits and ensures all practices and implementations meet required standards.
- **Incident Manager (SFIA: Incident and Service Request Management, GDS: Incident Manager):** Handles security breaches and mitigates damage, ensuring quick recovery and continuity of services. Manages the overall incident response plan including preparation, detection, and recovery.
- **Cloud Security Analyst (SFIA: Information Security, GDS: Technical Analyst):** Monitors cloud systems for security threats and analyses security incidents. This role plays a critical part in the continuous assessment and improvement of security measures.
- **DevSecOps Engineer (SFIA: Systems Development, GDS: DevOps Engineer):** Integrates security practices into the DevOps lifecycle to ensure secure software development and deployment. This role is key in automating security within CI/CD pipelines for efficient compliance and robust security.

Mapping to SFIA

Summary of the key SFIA Skills that align to this service.

Role	SFIA Skill Group	Likely SFIA Grade Range
Security Architect	Information Security	Grades 5-7
Security Engineer	Systems Installation/Decommissioning	Grades 4-6
Compliance Manager	Quality and Compliance Management	Grades 5-7
Incident Manager	Incident and Service Request Management	Grades 4-6
Cloud Security Analyst	Information Security	Grades 4-6
DevSecOps Engineer	Systems Development	Grades 5-7

For the SFIA roles and grade ranges included in the table, please refer to the official Skills Framework for the Information Age (SFIA) guidelines. More details and descriptions can be found at SFIA Foundation. Copyright Notice: © Skills Framework for the Information Age Foundation. All rights reserved. The use of information provided in this document should be in compliance with the guidelines established by the SFIA Foundation at sfia-online.org.

Scenarios

We consider a few scenarios/projects where this service could support agencies and departments with their cyber security posture/risk position across their programme/digital solution delivery:

Rapid Integration of Cyber Controls for Beta Service: A digital service nearing the end of its development cycle requires a comprehensive security review to meet stringent compliance standards (GDS, NCSC, Cyber Essentials) before going live.

- Critical Roles: The Security Architect aligns the requirements to the right frameworks to identify vulnerabilities and ensure compliance; the Compliance Manager oversees the alignment of the service with necessary regulatory standards.
- Benefits: The service advances to live deployment with enhanced security measures, ensuring regulatory compliance and a reduced risk of cyber threats.

Secure Mobile Government-to-Citizen Service : A new mobile service handling sensitive personal data for government-citizen interactions needs to establish stringent security controls from the start.

- Critical Roles: DevSecOps Engineer integrates security practices into the development lifecycle to safeguard data; Security Analyst conducts regular threat assessments to adjust security measures dynamically.
- Benefits: The service maintains high integrity and confidentiality of user data, bolstering public trust and mitigating potential cyber risks.

Enhancing Security in Containerized Public Cloud Deployment: An existing service deployed on a public cloud platform using containers requires security enhancements due to identified vulnerabilities and recent security incidents.

- Critical Roles: Cloud Security Specialist revises and strengthens the security architecture; Incident Manager enhances response strategies and incident handling protocols.
- Benefits: Strengthened security protocols reduce the service's vulnerability to attacks, ensure continuous compliance with the latest security standards, and maintain operational integrity.

Security Overhaul of an Existing Digital Service: A well-established digital service needs a security upgrade to address new compliance requirements and emerging threats.

- Critical Roles: Security Engineer applies the latest security technologies and practices to protect against advanced threats; Compliance Manager ensures all changes meet strict regulatory standards.
- Benefits: Updated security measures and compliance protocols increase the service's resilience against cyber threats, ensuring sustained user confidence and regulatory approval.

Cloud Support Service Details

Cloud Support Service Details

Planning

How the planning service works: Our services include comprehensive planning capabilities, to assist in the implementation of your hosting and software solutions. Our services encompass business analysis, solution design, and security architecture, to ensure a thorough preparation phase for implementing the right solution(s). We believe in a collaborative approach, acting as a 'critical friend' to guide, advise, and share our deep experience throughout the planning and implementation phases.

Adopting an agile, risk-based methodology, we will follow an iterative planning approach, using standard tools/frameworks to ensure transparency, effective communication, and confidence in the implementation process. Our strategy aligns with the Government Digital Service (GDS) Service digital lifecycle, covering Discovery, Alpha, Beta phases. This model focuses on user-centric, outcome-based, agile delivery, working closely with client teams to achieve common objectives.

Each project is supported by a dedicated account lead and project manager, along with highly skilled technical skills tailored to your project's needs. This structure is designed to maintain focus, provide leadership, and support your organisation through the intricate processes of design, delivery, implementation, and adoption.

These planning services extend across all of our cloud offerings, providing a holistic support framework designed to facilitate a smooth transition to cloud technologies, ensuring objectives are met efficiently and securely.

Setup and migration

How the setup or migration service works: Our cloud service facilitates a smooth migration to your preferred cloud environment, be it public, private, or sovereign. Led by expert cloud architects and engineers, we begin with a detailed setup phase, analysing your current infrastructure to identify and mitigate risks for a seamless transition.

We employ the Government Digital Service (GDS) Design Approach, moving through Discovery, Alpha, and Beta phases, guided by the GDS Technology Code of Practice. This ensures a well-planned migration. Our methodology includes the Proof of Concept (POC), Pilot, and Minimum Viable Product (MVP) approach, allowing us to identify and solve issues early on, ensuring quality and continuity during delivery.

We assign a dedicated account/solution lead and a technical specialist as your single point of contact during delivery. These key team members collaborate closely with your team, offering guidance, confidence and facilitating knowledge transfer to ensure the success of your migration. Our personalised approach aims to not just transition but transform your journey to the cloud, equipping you for success in the digital age.

Quality assurance and performance testing

How the quality assurance and performance testing works: Our services include integral and comprehensive quality assurance and performance testing capabilities. Our approach is grounded in Agile methodologies, ensuring that our services not only meet but exceed the key technology, security and public sector standards , ensuring alignment with frameworks such as Cyber Essentials, CIS, and NIST 800-53 as required. Our risk-based strategy in design, build, and delivery phases guarantees that the solutions adhere to business, service, data protection, and security requirements efficiently and effectively.

In our delivery process, we will follow an agile methodology to foster visibility, and velocity, enabling delivery teams to work closely with stakeholders. This collaborative approach ensures that requirements are met, quality is maintained, risks are mitigated, and user needs are understood. Our Continuous Integration/Continuous Delivery (CI/CD) practices employ a test-driven approach to platform, solution, and application development, incorporating Compliance-as-Code to enhance quality and ensure successful delivery.

At the core of our service delivery is our monitoring system that ensures all functional and non-functional requirements are tracked and correctly prioritised. Using shared tooling, stakeholders and managers can monitor delivery, using a comprehensive testing approach, providing clients with confidence that their cloud solutions are reliable, secure, and aligned with their specific needs and objectives.

Training

How the training service works: Our cloud services encompass a comprehensive range of training options, designed to support client needs throughout the design, build, deploy, testing and assurance phases. Utilising a DevOps / DevSecOps approach, our training is geared towards enhancing understanding and proficiency to help drive compliance and meet regulation needs through practices like Infrastructure as Code or a test-based development approach. Training delivery is tailored to the project and client needs, offering flexibility through various formats such as remote/distance learning, webinars, computer-based training, or traditional lecture/theatre-style presentations. This flexibility ensures that participants receive training in a manner that best suits their learning preferences and logistical requirements. Our service(s) are aligned with the platforms and solutions we offer, covering critical areas such as Platform Hardening, Boundary Controls, Network Design, Data Protection and Assurance (covering data at rest and in transit), Identity and Access Management & Authentication, Continuous Compliance, and Platform as Code. This ensures that training is not just about theoretical knowledge but is deeply connected to the practical applications and real-world solutions, empowering participants to effectively apply what they have learned in the delivery of the services.

Ongoing support

How the support service works: Our comprehensive support for cloud hosting and software services is designed to meet the diverse needs of our clients across the various platforms, applications, and user needs. We offer a tailored support structure, encompassing 1st, 2nd, and 3rd line support options, leveraging both UK/Sovereign and offshore capabilities to ensure optional global coverage and expertise. Our flexible model includes on-site support where necessary, ensuring that we can meet the specific requirements of each client.

Support availability ranges from standard working hours to extended coverage, including both a "10x6" and "24x7" support models. Clients can access support through a variety of channels, enabling them to choose the most convenient and effective method for their situation. We also offer integrated support options, allowing for seamless collaboration within a multi-cloud, multi-vendor landscape, whether as part of an integrated resolver group or within a federated Service Integration and Management (SIAM) structure.

Our ITILv4 service design is focused on delivering the highest quality of service management and availability. By understanding the unique challenges and objectives of each solution, we tailor our support service to provide reliable, efficient, and effective solutions to our clients, ensuring reliability, and efficiency from their hosting and software services.

Service scope

Service constraints: Cloud Support Services will be delivered both locally and remotely as required to meet the goals. To facilitate better understanding, and improve knowledge transfer, we will always look to ensure a significant component of the services are provided on site, and Face-to-face where possible/appropriate. Delivery will normally be delivered during normal working hours, with skilled experienced staff, with appropriate vetting to meet business needs. Extended support capabilities are available on-request.

User support

Support response times: Three levels of support are provided; UK working Hours, extended - "6x12", and “24x7”. 1st-Line queries raised by registered users by email, web-chat, directly via portal/phone. 2nd line support responses provide support to named staff /incident agents . 3rd Line support queries raised by named support agents, with an additional option to enable direct contact to engineers if required. P1 & P2 incidents have an SLA to be assessed and responded to within 30mins of notification/alert. The SLA for P3 & P4 incidents is 4 hours to confirm assessment/scheduling. P5 or Change Requests are responded to within 2 working days.

Phone support availability: 9 to 5 (UK time), Monday to Friday

Web chat support availability: 24 hours, 7 days a week

Support levels: Our cloud support includes an Account Manager as your Single Point of Contact (SPOC) for efficient escalation. We offer three support levels tailored to your needs: standard, extended, and 24/7 coverage, with P1/P2 incidents receiving 24/7 response, ensuring urgent issues are promptly addressed. Users can report 1st Line support issues through email, web-chat, the portal, or phone. 2nd Line support, for more complex issues, is accessible to support staff via the same channels. 3rd Line support, for the most technical challenges, is available to named agents with the option for direct engineer contact. We prioritise incidents based on severity: P3 and P4 within four hours for triage, and P1 and P2 incidents are responded to within 30 minutes. P5 incidents or change requests are addressed within two working days. A named Solution or Technical Lead complements the Account Manager, ensuring comprehensive service delivery. Our incident response framework is clearly defined from P1 to P5, designed for rapid and effective resolution. For detailed information on support options and pricing, please refer to our Service Pricing Document.

Social Value

Fighting climate change

Our cloud services are meticulously designed to support the government's social value agenda, especially in the battle against climate change. Recognising the environmental impact of digital services, we are committed to sustainable practices. This begins with an assessment at the start of each service delivery, pinpointing areas for consideration, and establishing relevant goals and KPIs. This evaluative process, shared with the client, outlines key stakeholders and responsibilities, ensuring a transparent and collaborative approach from the outset.

Our services are designed to leverage green initiatives, services and data centres available to public sector clients, prioritising energy efficiency,and reducing carbon footprint of digital activities. By offering solutions that encourage clients to move to cloud-based systems, we aid in the delivery of environmental goals, providing tools for energy consumption monitoring and reduction.

We pledge ongoing improvement in sustainability, aligning our operations with the latest environmental standards. This commitment includes regular assessments against the project's KPIs and quality criteria, ensuring we meet our environmental objectives and contribute positively to the government's agenda against climate change. Through this dedicated approach, we not only deliver high-quality cloud services but also foster environmental stewardship, reinforcing our role in the global effort to mitigate climate change. A statement of our Social Value and Climate Change policy is published on our website.

Covid-19 recovery

Our cloud services are designed to align with the government's social value agenda on supporting recovery efforts from the Covid-19 pandemic. Understanding the pivotal role technology plays in post-pandemic recovery, we begin each project with Social Value assessment, identifying how our services can best contribute to recovery objectives. This process includes setting clear goals and KPIs in consultation with our clients, pinpointing key stakeholders, and assigning responsibilities to ensure a collaborative approach throughout the delivery.

We recognise the critical need for digital infrastructure that not only facilitates remote work and education but also strengthens the resilience of public systems and services. Our solutions are crafted to enhance connectivity, scalability, and security, enabling organisations to adapt swiftly to changing needs and ensuring uninterrupted service delivery to the public. By providing robust, scale-able cloud infrastructure, we empower public sector organisations to efficiently manage increased demands on services, facilitate remote learning and working, and support the digital transformation of public services, contributing significantly to the Covid-19 recovery process.

Moreover, our commitment to ongoing assessment and improvement ensures that our projects remain aligned with the evolving recovery landscape, allowing us to adapt strategies and objectives as necessary. Through these dedicated efforts, our cloud services not only meet the immediate needs of our clients but also support broader recovery goals, fostering resilience, innovation, and inclusivity in the aftermath of the Covid-19 pandemic. Our approach underscores our commitment to contributing positively to the government's social value agenda, ensuring that our technology solutions play a key role in the national recovery effort.

A statement of our Social Value policy is published on our website.

Tackling economic inequality

Our cloud services are intricately designed to align with the government's social value agenda including the focus on tackling economic inequality. At the core of our approach is the initial Design phase, which includes an assessment where we identify opportunities to support economic inclusivity. This phase identifies and sets specific goals and KPIs, engaging clients and stakeholders in a transparent dialogue to ensure shared objectives are well-defined and achievable.

By providing scale-able and accessible cloud solutions, with embedded knowledge transfer, we aim to democratise access to technology, enabling public organisations of all sizes to leverage advanced digital tools and services. Our approach looks to bring small enterprises (SMEs) and startups to the delivery, fostering innovation, agility and value-for-money across delivery. Our cloud solutions support remote working and learning, essential elements in modernising employment and education opportunities, thus contributing to reducing economic disparities.

Our commitment extends beyond initial implementation; we ensure ongoing assessment against the project's KPIs and quality criteria, focusing on enhancing digital literacy and access. Through this continuous evaluation, we aim to adjust and refine our strategies to meet evolving needs, ensuring our services remain effective in promoting economic equality.

Furthermore, by facilitating the digital transformation of public services, we support more efficient resource allocation and service delivery, which in turn can lead to improved economic conditions for under-served communities. Our cloud services not only provide the technological backbone for innovation and growth but also embody our dedication to fostering an inclusive digital economy, directly contributing to the government's efforts to tackle economic inequality. A statement of our Social Value policy is published on our website.

Equal opportunity

Our organisation and service delivery is crafted to meet the government's social value agenda, particularly in promoting equal opportunity. During the design stage, requirements with initial assessments look to identify strategies that will support or champion diversity and inclusion, setting clear goals and KPIs within the delivery. This approach aims to ensure our projects support gender racial and sexual equality, through equitable recruitment practices, actively seeking to eliminate bias, and support the fostering of a diverse delivery team that reflects the communities we serve.

We leverage our cloud own technologies to create more inclusive work environments, enabling flexible working arrangements that accommodate diverse needs and life circumstances. This flexibility is crucial for supporting all individuals, ensuring that everyone has the opportunity to contribute to and benefit from digital transformation.

Our internal and project-related processes are designed to encourage and support professional development for all team members, with a particular focus on underrepresented groups. We implement mentorship programs, professional development opportunities, and inclusive leadership training to ensure that every project member (both client and supply side) can advance and thrive. By actively addressing gender bias, race, and sexual equality within our workforce, we not only enrich our company culture but also enhance the quality and creativity of the solutions we provide to clients.

In alignment with the government's agenda, our services play a role in breaking down barriers to equal opportunity, using technology as a force for social change. Through deliberate and thoughtful practices in recruitment, project execution, and ongoing workforce development, we are committed to fostering an environment where diversity is celebrated, and every individual has the chance to succeed.

A statement of our Social Value and Equal Opportunity policy is published on our website.

Wellbeing

Aligning delivery with the social value and Wellbeing agenda.

In every service delivery, During the mobilisation stage, we will initiate with simple assessment, pinpointing how our offerings and delivery approach can enhance the wellbeing of both the delivery and the client's team. This involves setting requirements, revising delivery processes, setting goals and aligning KPIs , so that focus is on creating a positive, supportive work environment, fostering a sense of community and belonging among all stakeholders.

We understand that the wellbeing of the delivery team is closely linked to the work environment and access to supportive technologies. Our ways-of-working and cloud solutions facilitate remote and flexible working arrangements, allowing individuals to balance professional responsibilities with personal health and family commitments. This flexibility is crucial in reducing stress and promoting a healthier work-life balance, contributing significantly to overall wellbeing.

Our delivery process emphasises collaboration and inclusion, ensuring that all team members feel valued and heard. We engage in regular dialogue with our clients and their teams, offering training and support that empower them to make the most of the cloud services we provide. This approach not only enhances technical skills but also boosts confidence and job satisfaction, which are essential for mental and emotional wellbeing.

Our delivery approach includes the ongoing evaluation and feedback mechanisms, allowing us to adjust ways of working and processes to better meet the needs of all team members. By prioritising wellbeing in our service delivery, we aim to create a more positive, productive, and healthy work environment, directly supporting the government's agenda to promote wellbeing across the workforce. Through these concerted efforts, we contribute to a culture that values and nurtures the wellbeing of every individual involved.

Strategic Advisory across Public Sector

highways england	Highways England	Service, Design & Architecture to support requirements, service design and compliant procurement of business critical “cloud” solutions.
Driver & Vehicle Licensing Agency	Driver and Vehicle Licensing Agency “DVLA”	Client side specialist team driving the Cloud and Security Transformation programme (“PACT Exit”), covering Architecture, Security, Service Design
SLC Student Loans Company	Student Loans Company	Technical & Strategic Service design. Requirements, strategic alignment, supplier selection & management. Delivery of cloud delivered security compliant CD/CI platform to support distributed new-generation application design
Border Force	Home Office Border Force	Design, develop, test, deploy and operate a Secure solution using DevOps * CD/CI to support capturing of passengers leaving by Air & Sea ports (“Exit Checks”)
NHS Business Services Authority	NHS Business Services Authority	Cloud Transformation requirements to support deployment of new UK major digital services. Security requirements and alignment of Service to Cloud and Security needs.
Department for Work & Pensions	Department for Work & Pensions	DWP Business and IS Strategy. . Delivery and implementation options, Prioritisation of strategic initiatives, phasing and funding. Analysis of strategic fit of in-flight programmes with the vision. Providing expert advice and leadership in IS plans for DWP
HM Revenue & Customs	HMRC/Inland Revenue	Provide thought leadership and entrepreneurial skills “strategic million” team.: Visioning of the department in five years time, architectural and business solutions needed to achieve the business goals
	Fd Army	Organisation Design and change delivery. People, Process & Technology changes to measure, manage and enhance delivery of a wide range of strategic projects to create and demonstrate an efficient and effective 3* HQ.

IT Enabled Change

Security

Sourcing

Service Transformation

Cloud-Dog Solutions
Viewdeck Engineering Limited
124 City Road,
London,
EC1V 2NX
+44(0) 203 020 0034
sales@cloud-dog.io