



G-Cloud 15 Service Definition

Cloud Platform Operational
Support and Application Support
Lot 3 Cloud Support

20/01/2026



Contents

1	Introduction.....	1
1.1	Triad Company Overview	1
1.2	Value Proposition	1
1.3	What the Service Provides	2
1.4	Overview of the G-Cloud Service	3
2	The Service in Detail.....	4
2.1	Service components	4
2.1.1	Core service functions	4
2.1.2	Supporting service functions.....	4
2.1.3	Service management	5
2.2	Service Delivery Methodology.....	6
2.3	Technical Environments and Tools	7
2.4	Service Levels	8
2.4.1	Sample Severity Levels	8
2.4.2	Sample Response Times	8
2.5	Cultural Fit	9
3	Data Protection	10
3.1	Information Security and Assurance	10
3.2	Data Back-Up and Restoration	10
3.3	Business Continuity Statement/Plan.....	10
3.4	Privacy by Design	10
4	Service Provision.....	11
4.1	Ordering and Invoicing	11
4.1.1	Ordering	11
4.1.2	Invoicing	11
4.2	Pricing Overview	11
4.3	On-Boarding and Off-Boarding	12
4.3.1	On-boarding	12
4.3.2	Off-boarding.....	14
4.4	Customer Responsibilities.....	14
4.5	Deliverables and Outcomes	14
4.6	Termination Process.....	14
5	Our Experience	16
5.1	Case Studies.....	16
5.1.1	HMCTS Crime Programme	16
5.1.2	Home Office Application Container Platform	16
5.2	Customers	17
5.3	Contact Details.....	17
6	Appendix 1 - Associated Services	18

1 Introduction

1.1 Triad Company Overview

For over 35 years, the UK public sector has been trusting Triad to define, design and deliver digital solutions. From the start of the “as a Service” model, we have encouraged and supported deployment to the cloud. We have established a strong track record across Central Government, Local Government, the Health sector and Policing. Our customers include the Office for Product Safety and Standards (OPSS), Foreign, Commonwealth and Development Office (FCDO), Met Office, Medicines and Healthcare products Regulatory Agency (MHRA), Cabinet Office, Ofgem, the Ministry of Justice (MOJ), the Home Office, the Department for Energy Security and Net Zero (DESNZ), Department for Business, Energy and Industrial Strategy (BEIS) and the Department for Transport (DfT).

When delivering cloud-based services, Triad adheres to best methods and practices for architecture and application design, build, test, deploy and operate. Early adopters of Agile, Triad has extensive experience of implementing DevOps and GitOps ways of working to underpin the “continuous everything” principle.

1.2 Value Proposition

To deliver excellent citizen-facing or back-office public services in the cloud, your system environments must be provisioned and managed efficiently and effectively. You need your development, test and production platforms to be resilient, performant and secure.

At the same time, you need your applications to be maintained so they keep pace with new requirements, enhanced functionality and product upgrades and updates.

All this must be done in accordance with relevant strategy, policy and strict governance, standing up to continuous scrutiny.

Triad has the experience and expertise to consistently set up, operate and support platforms and applications bringing benefits including:

- High reliability to build confidence with citizens, internal users and development teams
- Optimised performance to increase productivity
- Optimised costs to deliver value to the taxpayer
- Increased security to reduce the risk of cyber attack and compromise.

We achieve this by collaborative planning and applying best practice through all stages of a product or service lifecycle. We particularly focus on setting up a robust DevOps environment (combining software development and IT Operations) to shorten development times and provide continuous delivery with high software quality.

Constant learning and continuous improvement underpin everything we do, so the journey to excellence keeps going for as long as you engage us.

Our customers tell us they value our high integrity, accountability and openness. They highlight that we “go the extra mile”, working in their best interest and being their critical friend. It is always our intention to provide you with up-to-date and cost-effective cloud platforms and applications.

1.3 What the Service Provides

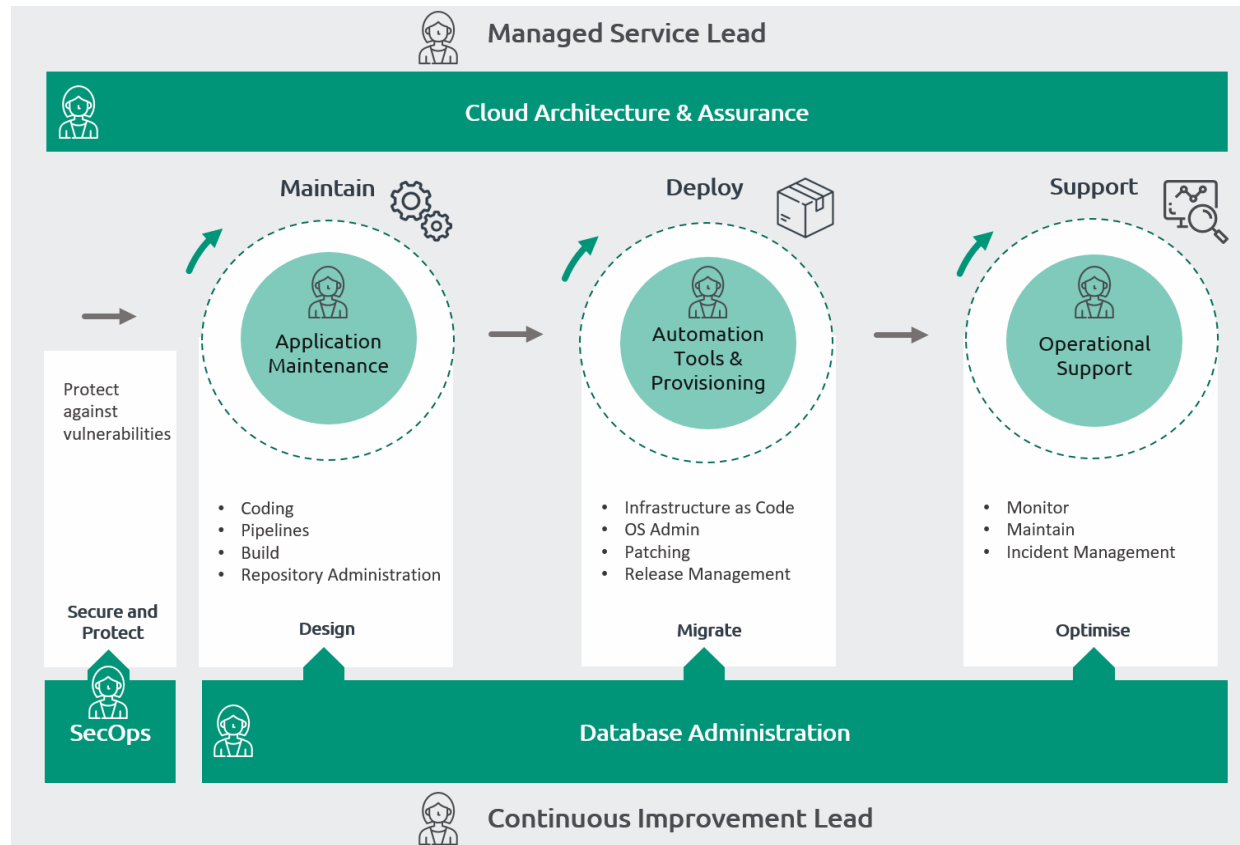
With this G-Cloud Cloud Platform Operational Support and Application Support service, you can engage Triad to support your cloud platform and application environment in any of the following scenarios:

- Architecting new cloud-based development, test and/or production environments including DevOps, GitOps and automation tools
- Building and deploying new environments
- Managing, maintaining and optimising built environments
- Transitioning between environments
- Applying optimum security through SecOps and DevSecOps
- Proactive monitoring of platforms and applications
- Deploying, maintaining and supporting applications
- Administering and managing databases.

You may want help with some or all of the above – we can provide specialist consultancy or complete managed teams. Whatever your platform and application support needs, you are in experienced hands with Triad.

1.4 Overview of the G-Cloud Service

The diagram below shows the key components of the service, which are described fully in Section 2.



Triad's optimised team structure for effectively managing cloud-based application services

*Figure 1: Structure of a fully managed Triad platform and application support team
Bringing 35+ years' solid experience delivering resilient, performant and secure environments*

2 The Service in Detail

2.1 Service components

2.1.1 Core service functions

The service illustrated in Figure 1 comprises three core functions: Application Maintenance, Automation Tools and Provisioning, and Operational Support. These functions collectively create a DevOps environment. Triad encourages the move towards a GitOps paradigm ensuring entire platforms and systems are described as code in one place with full traceability of changes driven through the pull request process.

When providing a managed team, each function has a dedicated team lead. Key responsibilities of each function are:

- **Application Maintenance:**
 - Code-level application maintenance
 - Continuous integration and continuous delivery/deployment (CI/CD) and build pipeline maintenance
 - Management of repositories and built artefacts/registries
- **Automation Tooling and Provisioning:**
 - Infrastructure as Code (for example, Terraform, Ansible, Cloud Formation/Azure Resource Manager (ARM) Templates)
 - System administration (Operating System patching, configuration)
 - Deployment tooling installation and maintenance
- **Operational Support:**
 - System monitoring and maintenance of frameworks, events and alarms
 - Issue and incident management and escalation
 - Application deployment.

2.1.2 Supporting service functions

The three core functions are supported by cross-cutting capabilities in Security Operations (SecOps) Cloud Architecture and Assurance, Continuous Improvement and Database Administration. Each function can be scaled up or down, in or out to respond to programme demand. For full teams, each function may require a team leader. Key responsibilities of each function are:

- **SecOps:**
 - Advising, securing and monitoring live and non-live environments

- Working collaboratively across the wider programme teams in a 'DevSecOps' culture to avoid security becoming a 'blocker' to delivery
- **Cloud Architecture and Assurance:**
 - Best practice design and reference architecture design for Software, Infrastructure and Platform as a Service (SaaS/IaaS/PaaS)
 - Architectural assurance and design support
- **Continuous Improvement:**
 - Key Performance Indicator (KPI) and Service Level Agreement (SLA) reporting
 - Identification of improvement opportunities and driving change
- **Database Administration:**
 - Database design, optimisation and migration
 - Installation, configuration and maintenance.

2.1.3 Service management

To ensure success and customer satisfaction, teams delivering this service are led by a **Managed Service Lead** (a senior Triad consultant), who works closely with a **Client Lead** (a senior Triad manager). The MSL is responsible for monitoring and managing day-to-day service performance across the teams on-site. The Client Lead provides governance oversight and supports the Managed Service Lead. Key service management benefits include:

- **Performance management:** full accountability for performance of the individuals and the teams, thus reducing the risk and management burden to you.
- **Consistent approach:** by creating and promoting common practices, both within our team and across different business services, we will achieve consistency and reduce duplication. Employing Triad permanent consultants will embed role models to guide and coach other team members in excellent practices.
- **Flexible resourcing:** through regular meetings with you and with our teams on the ground, we will forecast future resource requirements. We can increase or decrease resource levels and adjust skill types to optimise costs and capability.
- **Fast mobilisation:** we use our collaborative onboarding processes and invest in induction, training, clearance transfer (where applicable) and facilities provisioning to get teams and new team members up and running quickly to minimise learning time and maximise productivity.
- **Continuous improvement:** we constantly learn through retrospectives with you to identify areas for improvement. We also consult with the wider Triad team to bring best practice from other engagements to benefit you.

We will typically convene two regular meetings:

- **Weekly operational Service Checkpoints:** where your project manager(s) and the Managed Service Lead will assess the service performance against established KPIs and SLAs, and review next actions and risks, assumptions, issues and dependencies (RAID). Using the principle of Plan, Do, Check, Act, these will be open and transparent meetings where service delivery issues can be highlighted and speedily addressed.
- **Monthly Client Relationship Management (contract review) meetings:** where your senior management team and our Client Lead have the opportunity to monitor and shape the strategic aspects of the service, whether they are issues, challenges or opportunities.

2.2 Service Delivery Methodology

We are flexible in our approach, yet robust in our advice on the models that we know work well. In keeping with DevOps philosophy, we prefer to follow Agile methods and practices but are conscious that you may prefer, or have in place, a different approach. We do not force you to work to an unchangeable, predefined, delivery model; we work with you to tune your methodology, adopting only what adds value.

Throughout service delivery, we include all relevant parties to checkpoint risks, issues and dependencies and agree mitigation measures. We report and review with appropriate frequency to maintain service performance and are honest and clear about challenges.

This service may be used to provide short-term support to existing teams or a complete service over a longer period. Whatever the profile, we are mindful the service may transition back to your own staff or another third party in the future. We therefore include a continuous knowledge transfer process in our service delivery as shown below.



*Figure 2: Structured knowledge transfer with continuous learning and handover
An end-to-end process deployed successfully at the MOJ and the Home Office*

Throughout service delivery, we will maintain accurate records in accordance with agreed working methods and build documentation of systems, processes, historical incidents and outstanding issues.

All aspects of the work that our staff undertake will be shared with the appropriate members of your wider teams, both in terms of documents, code, workshops and meetings. Our approach will be to ensure that your members of staff, through our shared experience, will know as much about the services as do our staff.

Taking this approach will not only help accelerate delivery and provide true Agile flexibility within the team but will also minimise the amount of formal handover required at the end of our engagement.

2.3 Technical Environments and Tools

Triad has experience of working in private cloud environments and the most popular public clouds including Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform and UKCloud.

To maximise productivity, we make use of collaborative tools such as JIRA, Confluence, instant messaging and other digital communications.

Within these environments, we have extensive experience of a wide variety of frameworks, tools, databases and languages and have listed some of the most popular below. This is not an exhaustive list, therefore if the one you require is not mentioned here, please contact us and we can advise as to our experience.

Languages	Databases
Java, JavaScript/ES5, Typescript, Solidity C#, HTML 5, VB.NET, CSS3, Ruby	PostgreSQL, SQL Server, MongoDB, Oracle, Elasticsearch
Frameworks / Standards	Continuous Integration & Testing
ASP.NET Core, .NET Core, .Net Framework, Razor, Blazer, Microservices Bootstrap, Angular, Spring, Spring Boot, REST and RESTful APIs AMQP, CQRS, JSON Web Tokens, Polly, Swagger GOV.UK and ICDS design systems Heroku Open Source	Jenkins Artifactory, GIT, JMeter, Nexus Selenium, Gherkin, Postman, aXe, OWASP ZAP, WAVE, JAWS, Voice Over, NVDA Cloud Native pipeline management: Azure DevOps, AWS CodeBuild, GCP Cloud Build, GitHub Actions, Bitbucket Pipelines
Middleware	Cloud Services
RabbitMQ	Google Kubernetes Engine (GKE) Azure Kubernetes Services (AKS) Cloud SQL, Azure SQL, Azure App Services AWS ECS, Lambda, Fargate, EventBridge, API Gateway

Other Tools/Products

Docker, Kubernetes, Kibana, LogStash, Stackdriver, Liquibase, Hibernate, Entity Framework, Terraform

2.4 Service Levels

We will discuss and agree Service Levels with you based on your operational requirements when we agree the G-Cloud Call-off.

2.4.1 Sample Severity Levels

The table below outlines a baseline set of severity levels which would form the basis of our initial discussions on your operational requirements and service levels.

Severity Level	Description
1	The supported application(s) are down or there is a major malfunction affecting all users. Users are unable to reasonably perform their normal functions. The specific functionality is mission-critical to the business.
2	Critical loss of functionality or performance in the supported application(s) resulting in a high number of users unable to perform their normal functions. There is an inconvenient workaround, or no workaround exists. The supported application(s) is usable but severely impacted.
3	Moderate loss of functionality or performance in the supported application(s) resulting in multiple users impacted in their normal functions. A convenient workaround exists, there is minor performance degradation and it has a limited impact to normal functions.
4	Minor loss of functionality in the supported application(s). There are workarounds and there is no impact to normal functions.

2.4.2 Sample Response Times

The table below outlines an initial set of response times from which we would create and agree the response times that meet your operational requirements and service levels.

Severity Level	Respond Within
1	1 working hour
2	1 working hour
3	2 working hours
4	1 working day

2.5 Cultural Fit

You will find our style collaborative and transparent, working alongside your own staff and other supply partners. We have a strong 'no-blame' culture. Our focus is to deliver operational excellence. Everyone has a clear role and responsibility, and we hold them to account in a constructive and supporting way, helping to identify and remove blockers.

You will benefit from predictability in planning, the effectiveness of common governance and reporting across all business services, as well as an upskilling of your staff to adopt new roles. By planning for handover and establishing solid ways of working from the outset, transitions into live service and business as usual (BAU) become embedded and not an afterthought.

3 Data Protection

3.1 Information Security and Assurance

To give you the confidence that Triad is committed to implementing robust information security and assurance, we commit to maintaining the following certifications:

- ISO9001:2015 for the provision of IT consultancy services
- Cyber Essentials and Cyber Essentials Plus
- The IASME Governance standard (self-certified)
- ISO27001 for defining, implementing, operating, and improving an Information Security Management System (ISMS).

We always consider information security and assurance requirements as a crucial part of running our business and delivering our services. We will build in and test appropriate security measures and controls, liaising with third parties where appropriate. If you require appraisal and assurance of your current systems and strategic advice on enhancements to better meet business need and/or reduce costs, our security consultants can advise you at executive and business stakeholder level.

3.2 Data Back-Up and Restoration

Data back-up and restoration (including customer data) are covered in our routine ISO-certified company procedures and are documented in our Business Continuity Plan.

On customer projects, we will always discuss your data back-up and restoration processes when we develop digital cloud services for you or with you. We will consider the nature of the data and any legal obligations, the architecture, your existing processes (including those provided by any cloud hosting provider or managed service provider) and any constraints. We will design and document a back-up and restoration process as part of the handover documentation and transfer the relevant knowledge, so you can be confident of operation. This will typically be your responsibility once the system is operational.

3.3 Business Continuity Statement/Plan

Triad has robust business continuity plans covering the whole company operation. We can provide you with details on request.

3.4 Privacy by Design

Triad is GDPR compliant and will design GDPR-compliant systems in place for you. To protect citizen data, we have security systems in place to ensure all data under our control is safe and secure. If your digital cloud service includes a requirement to have access to citizen data, we will become a data processor for the provision of the service. As part of the project initiation process, we will discuss with you what access will be given to data and show where we will be a data controller or a data processor. Based on this conversation,

we will put in place a data sharing agreement to ensure we are fully aware of how we should handle data on your behalf. We will also carry out privacy impact assessments to identify any risks to the data and any extra security we may need to ensure we comply with the data sharing agreement.

4 Service Provision

4.1 Ordering and Invoicing

4.1.1 Ordering

Orders for Triad services follow the procedures and processes outlined in our Quality Management System (accredited to ISO9001:2015). There are three defined stages: clarification, review and acceptance.

- Following any clarification requests from you, we will provide a written response based on your needs, which sets out our recommended solution. The response is subject to management review and approval
- When you accept the solution, we will agree a Call-off Contract with you
- Once we have received the Call-off Contract, we will accept it and initiate Project Kick-off protocols: we will appoint a Project Manager; create record repositories (including for reporting and monitoring), allocate resources and set milestones.

4.1.2 Invoicing

Using Triad's invoicing system and processes, we generate and promptly send accurate invoices in line with contracted payment terms and procedures.

The efficiency and accuracy of our invoicing is due to:

- Modern time capture software and applications driving invoice creation
- Automated reviews
- Regularly audited end-to-end finance processes.

Verification checks are made throughout the invoicing process.

Please contact accounts@triad.co.uk for further information.

4.2 Pricing Overview

Prices for this G-Cloud service will be based on your specific requirements and our assessment of your needs.

All prices will be based on the day rates provided in the rate card and our Pricing document attached to this service.

4.3 On-Boarding and Off-Boarding

4.3.1 On-boarding

On-boarding is designed to establish an effective team and common ways of working, governance and reporting as shown in the diagram below.

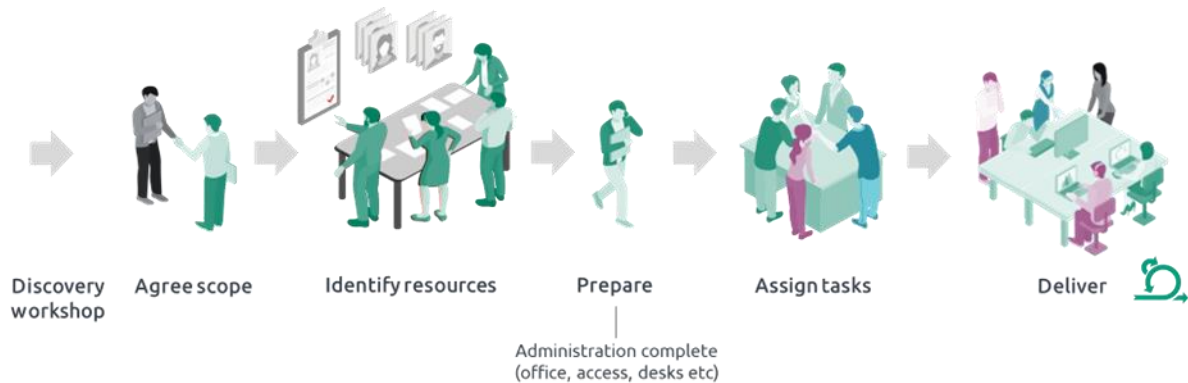


Figure 3: Triad's approach to on-boarding
Robust mobilisation processes combined with experience for rapid and effective service launch

Through collaboration with your staff and relevant supply partners, we agree a staged mobilisation plan. We execute the plan with transparency, reporting progress via regular meetings.

A typical mobilisation for a small team is set out below (we scale and flex this approach for larger engagements):

Week Minus 1 - pre-start

- Key resources join:
 - Managed Service Lead (MSL)
 - Operational Support Team Lead
 - SecOps Team Leads
 - Cloud Architect
- Key tasks:
 - Assess resource levels and handover tasks required
 - Identify key person dependencies and associated risks and opportunities to optimise resourcing
 - Agree handover plan with you and any incumbent suppliers

Week 1 - Discovery

- Key resources join:

- Continuous Improvement Lead
- Key tasks:
 - Gather full picture of architecture, development practices and delivery processes
 - Collaborate with other suppliers to agree common approach and transition plan for outgoing staff
 - Agree facilities and equipment and access to premises and systems
 - Agree governance, reporting structure and deliverables
 - Identify KPIs and define how KPI data will be sourced and captured
 - Gather KPI data and create KPI baseline
 - Prepare for on-boarding full teams
 - Build risk log and action mitigation

Week 2 to 5 - Handover

- Key resources join:
 - Core Operational Support team
 - SecOps team
 - Automation Tools and Provisioning team
- Key tasks:
 - Start KPI data recording
 - Execute agreed handover tasks
 - De-risk key person dependencies
 - Ramp up resource levels
 - Release incumbent(s) as appropriate

Service Delivery from Week 6

Each service handover is different, however, by week 6 we expect to be running at full velocity and will have already taken ownership of many aspects of the service delivery.

- Key tasks:
 - Continuous monitoring: KPI data captured and published on an ongoing basis.
 - Continuous improvement: process improvements identified and delivered
 - DevSecOps collaboration: team work together to enhance velocity
 - Operational excellence: cross-business 'Special Interest Groups' created to collaborate and share learning, standards and approaches.

The team leads and teams will be formed from our pool of high-calibre permanent staff and associates primed for rapid deployment. We ramp up resources only when they are needed, to provide you with the most cost-effective solution. Working with our in-house resourcing capability, we can flex up and down team sizes as appropriate to service demands.

All our consultants are cleared to BPSS standards and we maintain over 85% of our consultants cleared to SC level.

To on-board new consultants during service delivery, we will assign an experienced 'buddy' to provide introductions and a high-level induction.

4.3.2 Off-boarding

As described in Section 2.2, Service Delivery Methodology, we cater for professional off-boarding from day 1 by continuously following our three-phase knowledge transfer process.

At the build-up to a formal service handover, we will develop more formal knowledge-transfer suitable for new operational and support teams. Our approach to this will be twofold.

First, we will start early by giving briefings on the new service and, in the case of operations, ensuring that they have exposure to the architecture of these services.

Second, we will provide a handover documentation set, including all assets that our team has been working on, topped and tailed to ensure easy navigation and digestion. We will back this up with ad-hoc and formal walk-throughs of concepts and components. As part of this we will allow time for the teams we are handing over to, to come back with specific areas that they feel require greater clarity.

4.4 Customer Responsibilities

To help us build and operate a high-quality service, we will need you to designate key points of contact mapped to each of our team leads and governance roles.

Depending on the scope of the project, we may need you to provide facilities and equipment and access to premises and systems. We will agree this with you during Discovery.

4.5 Deliverables and Outcomes

We will agree specific deliverables and outcomes with you during the Discovery.

4.6 Termination Process

Termination is in line with the standard G-Cloud terms and conditions available as a separate PDF attached to this Digital Marketplace service. In summary, the notice period needed for ending the Call-off Contract is at least 90 working days from the date of

written notice for disputed sums or at least 30 days from the date of written notice for ending without cause.

5 Our Experience

5.1 Case Studies

Triad has a track record of delivering Platform and Application Support services within the public sector including at HM Courts and Tribunals Service (HMCTS) and the Home Office as described below.

Triad's strengths have ensured success on these examples and other engagements where an in-depth understanding of DevOps, DevSecOps and SecOps has been required. These include Ofgem's Energy Compliance Obligations 3 (ECO3) project, DfT's Greenhouse Gas Emissions System (GOS) project and the Metropolitan Police.

5.1.1 HMCTS Crime Programme

On the HMCTS Crime Programme this wide-ranging Platform and Application Support extended to a team of approximately 30 Application Support Engineers, DevOps engineers, Cloud Architects and Operation Security specialists, for production and pre-production/non-live Azure and historically UK Cloud environments.

Our Platform and Application Support services covered five areas:

- Application Maintenance and Support
- Environment Maintenance and Support
- Environment Enhancements
- Interface Management
- Production Security

We understood the importance of maintaining a focus on operational metrics to drive continuous improvement and having that as the focus of discussion with the client. The initial SLAs and KPIs were adapted to better capture and track real issues.

5.1.2 Home Office Application Container Platform

For the Home Office, Triad's Platform and Application Support team provided the Application Containers Platform (ACP) DevOps service in support of programmes that included Platforms & Optimisation and Securing our Borders. The solution which was hosted on the Amazon Web Services platform made extensive use of container technologies including Kubernetes.

Our management of these services included contribution to the clients' business reviews against key performance indicators and non-functional requirements.

5.2 Customers

Triad has delivered digital cloud services across the public sector for many customers including those shown below.



5.3 Contact Details

If you would like to discuss this service, or any of the other services offered by Triad in the Digital Marketplace, please do not hesitate to contact us for an informal conversation:

Tim Eckes
Client Services Director

Triad Group Plc
Huxley House,
Weyside Park
Catteshall Lane,
Godalming, GU7 1XE

t: +44 (0)1908 278450
w: www.triad.co.uk
e: gcloud@triad.co.uk

6 Appendix 1 - Associated Services

In addition to this Cloud Platform Operational Support and Application Support service, you can also purchase the following Triad services through the Digital Marketplace:

- Agile Consulting and Agile Coaching for Cloud Services
- Cloud Consultancy Services delivering Cloud Strategies and Digital Transformation outcomes
- Digital Cloud Service Design
- Cloud Architecture Services: Enterprise Architecture, Solution Architecture and Technical Architecture
- Cloud Design Assurance Service
- Agile Project Delivery: Full Digital Service Development and Continuous Improvement
- Cloud Programme Management and Project Management Services
- Cloud Service Delivery and Release Management
- Business Analysis and Digital Solution Design Service
- Cloud User Research (UR) and User Experience (UX) Services
- Digital Cloud Service Development and Project Delivery
- Testing and Quality Assurance of Cloud Services
- Intelligent Automation and Robotic Process Automation (RPA) in the Cloud
- Blockchain and Innovation Technologies for the Cloud
- Geospatial Cloud Services
- Microsoft Cloud Consulting, Delivery and Support Service
- Cloud Delivery Partner Service
- Cloud Artificial Service
- Cloud Cyber Service
- Knowledge and Information Management Cloud Service
- SharePoint Cloud Service
- Dynamics365 Cloud Service
- Power Platform Cloud Service
- Cloud Service for Policing: SC, DV, STRAP
- Cloud Data Service
- Cloud Data Science, BI and Analytics Service

- Cloud Migration Service
- Cloud Discovery Service
- Legacy Modernisation Service
- Ruby Cloud Migration Service
- Salesforce Consulting
- Electronic Patient Record (EPR) Advisory, Implementation & Optimisation
- LIMS & Digital Pathology Delivery and Optimisation
- DTAC & Clinical Safety (DCB0129/DCB0160) Advisory Service
- Shared/Connecting Care Record Enablement & Interoperability
- Health Tech & Med Tech Needs Assessment, Option Appraisal & Adoption.