Service 1: Managed Public Cloud

1.1 Service Overview

We provide a Managed Public Cloud service that embeds platform engineering capability within client organisations. The service promotes autonomy and accountability through best practice and automation, enabling application teams to self-serve infrastructure via a contemporary platform that is easy to use and support.

The service operates on a Platform-as-a-Service model, providing self-service infrastructure through standardised, tested, and secure patterns. This accelerates application team delivery while maintaining governance, security, and cost control.

1.2 Service Features

Infrastructure as Code (IaC)

- All infrastructure provisioned and managed via Terraform
- Reusable, tested modules for common patterns (compute, networking, data stores)
- Version-controlled configurations enabling audit trails and rollback
- Automated provisioning reducing manual errors and configuration drift

AWS Services Management

- Compute: EC2, ECS, Lambda, Auto Scaling Groups
- Networking: VPC, Elastic Load Balancing, Network Firewall, CloudMap
- Data: RDS, Aurora Serverless, RDS Proxy
- Security and Monitoring: Secrets Manager, CloudTrail, CloudWatch, AWS Inspector

Cost Management and Optimisation

- Infracost integration in CI/CD pipelines for pre-deployment cost visibility
- Automated resource cleanup (e.g., AMIs older than 90 days)
- Auto Scaling Groups for dynamic resource optimisation
- Tagging enforcement for cost allocation and visibility

Monitoring and Alerting

- CloudWatch alarms deployed via Terraform for proactive monitoring
- Centralised logging via CloudTrail for API audit trails
- AWS Inspector for continuous vulnerability assessment

1.3 Service Benefits

Benefit	Description
Reduces deployment times	Standardised Terraform modules and automated pipelines enable rapid, repeatable infrastructure provisioning in minutes rather than days

Reduces business risk and costs	Infrastructure as Code reduces configuration drift and manual errors; automated cleanup and right-sizing reduce cloud spend by up to 50%
Accelerates application delivery	Self-service platform model enables application teams to provision infrastructure without waiting for central IT
Improves governance and compliance	Version-controlled infrastructure with full audit trails supports regulatory and internal compliance requirements
Increases operational resilience	Auto Scaling and infrastructure patterns built for high availability reduce single points of failure
Provides cost transparency	Infracost integration and resource tagging give teams visibility of cloud costs before and after deployment
Enables faster incident resolution	Centralised monitoring and alerting reduce mean time to detection and resolution

1.4 Service Levels

Service Level	Commitment
Availability	99% uptime for managed infrastructure components
Support Hours (In-Hours)	Monday to Friday, 09:00 - 17:00 UK time (excluding public holidays)
Support Hours (Out-of-Hours)	Available, limited to runbooks supplied by individual teams
Incident Response	As agreed per engagement
Deployment Frequency	Capable of 12+ infrastructure deployments per day
Change Failure Rate	Target below 5% (current performance: 1.79%)

1.5 Hosting Options and Locations

All services are hosted on Amazon Web Services (AWS) within UK regions:

- Primary region: eu-west-2 (London)
- Data residency: All data remains within UK boundaries

AWS maintains ISO 27001, SOC 2, and Cyber Essentials Plus certifications for UK regions.

1.6 Data Backup and Disaster Recovery

The following backup approach applies to raw audit/event data. Backup approaches for other data stores (RDS, Aurora, etc.) are agreed per engagement based on data classification and recovery requirements.

Backup Architecture

Component	Approach
Backup Method	S3 Same-Region Replication (SRR) to dedicated backup account
Backup Location	Separate AWS account (eu-west-2) with restricted access controls
Retention	7 years (6 years + 1 for compliance)

Encryption	Server-side encryption using dedicated KMS keys per bucket (SSE-KMS), key rotation enabled
Integrity Validation	S3 Inventory comparison between permanent and backup buckets; replication validation jobs
Deletion Protection	Deletions not replicated to backup; S3 Object Lock with Governance Mode enabled
Recovery Point Objective (RPO)	Near real-time (seconds) via S3 replication
Recovery Time Objective (RTO)	Agreed per engagement based on data volume and recovery requirements

Security Controls

- Backup account isolated with locked-down access controls
- Explicit deny on all operations unless principal matches allowed role ARN
- TLS only, no public access
- Access logging enabled with GuardDuty for anomaly detection
- Object versioning enabled on both permanent and backup buckets

Monitoring and Alerting

- Replication failure alerts via CloudWatch metrics
- Unexpected file update alerts (outside of known repair processes)
- Unexpected deletion alerts for objects newer than retention threshold

Business Continuity

- Multi-AZ architecture with automated failover for critical workloads
- Documented runbooks and tested recovery procedures
- Recovery from backup account in event of data loss in primary account

1.7 Service Constraints

- Service limited to AWS cloud platform
- Customisation of Terraform modules supported through self-serve approach
- Third-party software licensing remains client responsibility
- Application code development and deployment is client responsibility; infrastructure support only
- Support provided during UK business hours only; out-of-hours support available at additional cost

1.8 Outage and Maintenance Management

- Planned maintenance communicated minimum 5 business days in advance
- Emergency maintenance communicated as soon as practicable
- Maintenance scheduled outside core business hours where possible

- Status updates provided via agreed communication channels (email, Slack)
- Post-incident reports provided for P1 and P2 incidents within 5 business days

1.9 Technical Requirements

Client technical requirements:

- AWS account with appropriate IAM permissions for service team
- VPN client software for secure access to managed environments
- Git repository access for Infrastructure as Code collaboration
- Communication tools (Slack or Microsoft Teams) for operational coordination