technogise

G-Cloud 15 (RM1557.15) Technogise UK Private Limited

Migration and Legacy System Modernisation Services

Service Definition

Dec 2025

Table of contents

1 Introduction

1.1 Document structure

This Service Definition document provides information about the services offered by Technogise under the G-Cloud 15 Framework. We have designed the document to help public sector buyers understand the functionality, security, pricing and management of our services. The document will clarify how to work with us using the framework, outlined in the following sections:

Service description	Operational delivery	Supplier information
Provides an overview of our cloud support services, outlining key features, benefits, delivery methodology and assurance measures, including security and compliance.	Details how our services are delivered under the G-Cloud 15 framework.	Summarises our company background, mission, relevant experience and how to procure our services through G-Cloud.

1.2 How to use this document

This document is intended to support buyers throughout their G-Cloud procurement journey, detailed below:

- To support early-stage evaluation, Section 2 outlines our service scope, approach and key benefits
- For due diligence and contract preparation, Section 3 provides details on onboarding, service levels, data management, support and exit procedures
- To ensure data protection and compliance, Section 4 describes our information-security practices, data handling standards and business continuity measures
- For supplier verification, Section 5 offers background information on Technogise, including relevant certifications and procurement routes

2 Service description

2.1 About our service

Our cloud support services transform outdated, expensive legacy systems that hold organisations back. By solving complex migration challenges, we enable clients to innovate and scale their services. During transformation, we keep business running smoothly, uphold compliance at every step and reduce technical inefficiencies. We provide expert cloud migration, cloud-native architectures and legacy system modernisation services. Specialising in zero-downtime transformations, we use proven engineering approaches to deliver enterprise-scale modernisation for regulated environments.

Under the G-Cloud 15 Framework, we provide cloud support services designed to enable public sector organisations to transition from outdated systems to modern, cloud-native architectures. Our target clients for this service are public sector organisations. For example, Local Authorities, the NHS and central government departments that need to upgrade or modernise their legacy systems, such as patient management or tax systems. We bring a proven track record in regulated industries across 25 countries and enterprise-scale applications serving millions of users. This includes financial services, gaming and e-commerce sectors.

2.2 Delivery framework

Supporting clients through the entire modernisation lifecycle, we deliver end-to-end cloud services. This includes:

- Discovery and assessment (4-6 weeks)
- Architectural design and planning
- Migration
- Implementation
- Consultancy
- Continuous integration and delivery
- Post-migration optimisation
- Team enablement and training
- Support and maintenance

Adding value, our Consultants work as embedded members within their client teams. This ensures our clients' staff can independently extend, maintain and optimise new systems after our engagement ends. For example, we combine hands-on pair programming, architectural design workshops and 'train the trainer' sessions.

Providing post-migration optimisation and support, our teams can be on hand. We follow the principles of 'you build it, you run it'. Whilst we are still on-site, the team continues to run the service and iteratively improve it. As a result of our approach, we have delivered the following client results:

- Reduced deployment times by **28%** - Finzy
- Improved conversion rates by **66.67%** - Bally
- Zero downtime migration with **100%** availability – Pine Labs

2.3 Service features / benefits

Discovery and assessment services

To accurately plan for a smooth cloud transition, we guide migration and modernisation strategies, identify the current system architecture, map dependencies and assess risks. Key activities include:

- Analysing systems comprehensively by performing capability analysis, reviewing enterprise architecture and conducting gap assessments
- Mapping dependencies
- Assessing risks

Migration planning

Moving workloads to the cloud with minimal disruption, we develop a detailed roadmap, analyse architecture options, plan compliance and create delivery roadmaps. This ensures operational continuity, maintains regulatory compliance and reduces migration risk. Key features include:

- Designing detailed migration plans
- Implementing risk mitigation strategies
- Establishing governance frameworks

Platform modernisation

Improving scalability and accelerating deployment, we transform legacy platforms into scalable, cloud-native architectures. To achieve this, we implement containerisation and adopt serverless technologies to future-proof architecture. Key features include:

- Transitioning to microservices
- Deploying container orchestration
- Implementing serverless patterns

Data migration

Preventing loss or corruption, data migration securely transfers and validates data. We audit, organise and validate data structures before and after migration to ensure data integrity, GDPR compliance, and minimise downtime. Key features include:

- Using secure transfer protocols
- Applying governance checks
- Performing reconciliation processes

Performance optimisation

Improving efficiency and cost-effectiveness in cloud environments, we conduct performance testing, plan capacity and apply cost optimisation strategies. This service reduces costs, maximises resource use and ensures high system reliability. Key features include:

- Configuring auto-scaling
- Executing load testing

- Applying FinOps practices

Team enablement

Equipping teams with the skills and knowledge to manage and optimise cloud service, we deliver training, provide documentation and transfer knowledge. This service empowers teams, reduces reliance on external support and accelerates issue resolution. Key features include:

- Training on troubleshooting (basic to advanced)
- Developing super-user capabilities
- Conducting optimisation workshops

Architecture design

To create robust, scalable and secure cloud-native architectures, we design microservices, define Application Programming Interface (API) strategies, and apply cloud-native patterns. This service delivers scalable designs, embeds security by design and aligns with cloud standards. Key features include:

- Producing architecture designs and diagrams
- Developing API integration strategies
- Applying best practice

Strangler fig implementation

To migrate legacy systems incrementally without disrupting services, we replace monolithic components with modern services in phases. This approach avoids downtime, controls migration pace and reduces operational risk. Key features include:

- Maintaining the coexistence of old and new systems
- Continuous validation during migration

Continuous Integration (CI)/Continuous Delivery (CD) pipeline development

Automating software delivery for speed and reliability, we design pipelines for build, test and deployment stages with compliance checks. This service accelerates releases, reduces human error and maintains compliance. Key features include:

- Automating deployments
- Integrating testing frameworks
- Continuously validating compliance

Integration services

Connecting new cloud services with existing systems seamlessly, we develop APIs, integrate systems and wrap legacy services. Key features include managing APIs effectively, implementing middleware connectors, and adapting legacy systems. This service achieves seamless integration, extends system life, and minimises disruption.

2.3 Service scope

- **Service Type:** Cloud Support Services
- **Add-on or Extension:** No – standalone professional service
- **Cloud Deployment Model:** Hybrid
- **Multi-Cloud Support:** Yes – designed to operate across multiple public cloud environments such as AWS, Azure and GCPup

2.3.1 Service Integration Capabilities

While offered as a standalone service, our Cloud Migration and Legacy System Modernisation service integrates seamlessly with clients' existing technology investments and can complement other G-Cloud services. Ensuring our modernisation approach enhances rather than disrupts existing capabilities, we work with established platforms and tools, including:

- AWS
- Azure
- GCP
- Kubernetes
- Jenkins

2.4 Service assurance and non-functional requirements

2.4.1 Service constraints and dependencies

Our services are delivered within the following standard constraints:

Client responsibilities

For us to successfully deliver our services, clients must provide us with timely access to the following before commencement:

- Key stakeholders to action requirements, approvals and sign-offs
- System credentials and permissions
- Existing system documentation and architecture diagrams
- Anonymised test data for development and testing
- Workspace collaboration spaces (physical or virtual)

Compatibility with other platforms

- Cloud platforms: AWS, Azure, Google Cloud Platform
- Container platforms: Docker, Kubernetes, OpenShift
- CI/CD tools: Jenkins, GitLab CI, GitHub Actions, Azure DevOps
- Monitoring: Grafana, Prometheus, ELK stack, Datadog
- Databases: PostgreSQL, MySQL, MongoDB, Oracle, SQL Server

Planned maintenance windows

Preventing bottlenecks, we deliver zero-downtime deployments where architecture permits. Our planned maintenance windows are:

- Standard maintenance each Saturday from 10 pm to 2 am (UK time)
- Monthly non-critical updates
- Emergency maintenance with 24 hours' notice

Limitations

- To maximise value from our service, we recommend a minimum initial commitment of 3 months
- When delivering services, our geographic coverage is primarily within UK and EU time zones
- To ensure knowledge continuity when delivering services, we will require a minimum of 2 Consultants
- Services requiring Developed Vetting (DV) clearance will require longer lead times

Staff clearances

The following staff clearances are available within our team:

- Baseline Personnel Security Standard (BPSS) clearance available for all UK-based Consultants
- Security Check (SC) clearance can be obtained for specific engagements
- Developed Vetting (DV) clearance support available through partnership arrangements

Notice period needed for changes

For any changes to the service, we will require the following notice periods:

Change	Notice period
Team scaling up	1 week (fast-track) or 2 weeks (standard)
Team scaling down	4 weeks
Scope changes	1 week (minor) or 2 weeks (major)
Contract amendments	2 weeks

2.4.2 System requirements

- Minimum bandwidth: 10 Mbps for effective remote collaboration
- Supported OS: Windows 10+, macOS 10.14+, Ubuntu 20.04+
- Browser support: Chrome 90+, Firefox 88+, Safari 14+, Edge 90+
- Development environments: Docker, Kubernetes, cloud-native tools
- Collaboration tools: MS Teams, Slack, Jira, Confluence compatible

2.5 Reselling

We do not resell any services outside those declared in our G-Cloud listing.

2.6 User support

To ensure you can quickly access help, resolve issues efficiently and maintain operational continuity, we provide a responsive, tailored support service. We have aligned our support model to ITIL principles, which we deliver through:

- Self-service resources
- Multi-channel helpdesk support and escalation pathways to technical specialists

2.7 Performance monitoring and metrics

Proactively managing our performance, we conduct structured performance monitoring processes aligned with ISO 9001 Quality Management standards. For each project, we will continuously monitor our service under the oversight of your named Account Manager. To monitor and log performance, we will:

- Agree on key performance standards at the beginning of the contract
- Maintain digital records that meet your reporting needs
- Provide you with regular updates in a format and frequency suited to your needs

At agreed points throughout the service, we will provide you with meaningful performance metrics tailored to our Service Level Agreements (SLAs). For continuous improvement, we will apply these insights to our service delivery.

2.8 Accessibility and usability

To meet government accessibility standards for all services, we prioritise accessibility-first design from the outset. All interfaces and documentation comply with WCAG 2.2 AA and EN 301 549 standards, enabling people with a wide range of impairments to use them effectively. As a result, our service meets recognised accessibility standards and can be adopted across the public sector without additional adjustments. Our approach includes:

- Supporting assistive technologies like screen-readers, screen magnifiers and alternative input devices such as keyboard only and voice commands
- Ensuring that content is perceivable and understandable by providing good contrast, clear navigation, logical structure, and semantic HTML
- Designing forms, controls and interactive elements so they are fully operable via keyboard or other assistive input devices
- Making downloadable documents, such as PDFs and Word documents, accessible where they are used to deliver services. This enables them to be read by screen-readers or provided in alternate formats
- Conducting ongoing testing and maintenance at key points and maintaining an accessibility change log alongside this. Key stages we may test accessibility include:
- Before releasing a new feature
- During development
- When there are significant changes
- Annually, as a minimum, using sample-based audits

2.9 How users work with our servers

2.9.1 Browsers

The service is accessible through any modern standards-compliant web browser. We support the latest versions of:

- Google Chrome
- Microsoft Edge
- Mozilla Firefox
- Apple Safari

We recommend enabling JavaScript and cookies for full functionality. Buyers are notified in advance of any changes to browser support.

2.9.2 Desktop application

A desktop application is not provided for this service.

2.9.3 Mobile

The service is optimised for mobile use and supports iOS and Android devices. Users can access it through the mobile-responsive web interface or, when available, via our dedicated mobile app.

2.9.4 Service interface

Promoting easy navigation and accessibility, our service provides an intuitive, role-based interface. All components are mobile responsive.

2.9.5 Integration and customisation

We recognise that each client will have unique requirements, so we customise our approach to meet those needs by:

- Understanding sector-specific requirements, including unique regulatory needs such as NHS data standards and local government requirements
- Scaling our team size and expertise according to the complexity of the system
- Adjusting the migration pace based on the acceptable risk levels of each client
- Offering flexible engagement models that range from fixed-price discovery to time-and-materials (T&M) implementation to accommodate budget constraints
- Providing fast-track options for clients with urgent modernisation requirements
- Adapting our knowledge transfer approach based on the current skills of the client's team

We provide integration options with the following systems:

Category	Detail	Supporting standards	Buyer/User Control
Integration capabilities	Message queuing: RabbitMQ, Kafka, Azure Service Bus; Legacy integration: SOAP, file-based, database-level integration	SAML 2.0, OAuth 2.0, OpenID Connect	Full control available
API availability and documentation	RESTful APIs and GraphQL support	Government Digital Service (GDS) API standards compliance	Full Access
Customisation / configuration	Flexible customisation across architecture design, migration approach, integration patterns, security controls, team composition, and delivery methodology to align with client enterprise standards and requirements	X GDS Service Standard, TOGAF, ITIL v4, ISO 27001, client enterprise architecture standards, open standards (REST, OAuth, OpenAPI)	Full control

2.9.6 Reliability and continuity

To ensure resilience and prevent downtime, we host the service across UK data centres. Our primary data centre storage is in London and Manchester. Providing continuity in case of any issues, we have backup storage in place at UK-based cloud regions, AWS EU-West-2 and Azure UK South. As a result, we guarantee 99.9% uptime. Minimising disruption, our Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO) are:

- **RPO:** Maximum 1 hour for critical systems, 4 hours for standard systems
- **RTO:** Maximum 2 hours for critical systems, 8 hours for standard systems

To provide you with flexibility, we can create custom Service Level Agreements (SLAs) tailored to your specific requirements.

2.9.7 Compliance and quality management

The standards and methodologies that underpin our service are:

- Faster results with flexibility for changes using Scrum and Kanban methodologies
- Continuous improvement, applying ISO 9001 Quality Management principles
- Integration support with TOGAF for enterprise architecture
- Minimal long-term costs with SOLID principles and clean code practices
- Rapid delivery with Extreme Programming (XP) practices
- Reliable, consistent support with ITIL v4 for service management
- Efficiency and scalability with Cloud Well-Architected Framework (AWS/Azure)
- Secure software by applying DevSecOps practices
- Faster debugging using Test-Driven Development (TDD)

Tailored to public-sector constraints, we have developed our **Technogise Tech Sherpa™** internal methodology. Our lightweight, delivery-focused approach is designed for cloud, data and software projects and is built on agile, continuous delivery and user-centred design. For example:

- **Delivering a strong client and end-user focus** in our design and delivery, we employ a comprehensive, user-centred approach. We align solutions with genuine end-user needs and pain points by starting with thorough user research
- To **continuously refine our solutions**, we incorporate regular user feedback into each sprint through our iterative delivery approach. Each sprint delivers working software, with first production deployments typically within 8-12 weeks of engagement start
- Ensuring **close collaboration** and seamless integration, our Consultants work alongside client teams using an embedded delivery model. To foster transparency and shared understanding, we facilitate regular workshops on architecture decisions, sprint planning and retrospectives
- **Promoting knowledge transfer** through hands-on pair programming, while regular demos and feedback sessions keep stakeholders engaged throughout the process. To enable effective face-to-face collaboration, we offer co-location options for critical project phases
- Supporting **ongoing communication**, we also use shared documentation tools, such as collaborative wikis and knowledge bases. Finally, we encourage joint problem-solving through architecture review boards and technical decision forums
- Delivering an **optimal client experience**, we conduct ongoing performance and user monitoring and support smooth transitions to new systems with our change management support. To continually adapt to user needs, we conduct beta testing programs, which feature gradual rollouts and feedback loops

3 G-Cloud alignment information

3.1 Section introduction

We deliver every G-Cloud engagement through a tailored, collaborative delivery model. Providing flexibility, we adapt this to each client's specific objectives, scale and governance requirements.

Ensuring clarity, accountability and consistent quality from mobilisation to completion, our approach combines structured project controls with the flexibility needed for rapid iteration.

This section explains how we will work together at each stage of delivery, from onboarding and configuration through to live operation, support and secure offboarding.

Our service follows a structured yet flexible approach using 4 phases:

Phase 1 - Discovery (Weeks 1-4)

We conduct a thorough system analysis to identify dependencies, compliance requirements and technical constraints. This includes stakeholder interviews, codebase analysis and infrastructure assessment. During this phase, we establish the foundation for audit logging and compliance automation, ensuring that GDPR, FOI and transparency standards are accounted for early. We embed a security-first approach that aligns with government data protection requirements.

Phase 2 - Design and planning (Weeks 5-8)

We create detailed migration architecture, select appropriate cloud services, design microservice boundaries and develop a comprehensive migration roadmap with clear milestones. Providing early value and maintaining budget flexibility, we incorporate zero-downtime migration strategies and support incremental delivery. Ensuring resilience and regulatory alignment, we refine security and compliance automation in the architecture.

Phase 3 - Implementation (Weeks 9+)

Using the strangler fig pattern methodology, we incrementally migrate components while maintaining system operation. Each iteration delivers working software with immediate business value. Allowing clients to see progress and value quickly, this phase activates the incremental delivery model. To accelerate migration and reduce manual effort, we leverage AI automation and AI software delivery. Throughout, we enforce audit logging and security-first practices throughout the development lifecycle.

Phase 4 - Optimisation and handover

To ensure client team independence and success, we conduct post-migration optimisation. This involves performance tuning, training and delivering comprehensive knowledge transfer. To build internal capability and reduce reliance on external suppliers, we focus on knowledge transfer. Ensuring the system is scalable, secure and efficient, we complete final checks.

3.2 Onboarding and offboarding processes

3.2.1 Onboarding

The onboarding process includes team introductions, stakeholder workshops and delivery kick-off, to establish clear expectations, roles and deliverables. Our typical onboarding timeline for standard engagements is 2 to 3 weeks. For urgent projects, we offer a 1-week fast track option and for complex projects, the timeline is 4 weeks, including security clearances. Ensuring that governance, data access and communication structures are in place, onboarding concludes when all stakeholders have approved the SOW and project initiation documents. An example of our typical onboarding steps is detailed below:

- **Week 1-2:** Execute the contract, introduce the teams and access provisions
- **Week 2-3:** Conduct stakeholder workshops and assess current state
- **Week 3-4:** Kick off delivery, plan sprints and communicate protocols
- **Ongoing:** For continuous improvement, we conduct feedback loops with regular client check-ins

3.2.2 Offboarding

To terminate the service effectively and smoothly, our structured offboarding process involves the following steps:

- **Month -2:** Initiate handover planning
- **Month -1:** Conduct knowledge transfer sessions and complete documentation
- **Week -2:** Conduct final system walkthrough and validate runbook
- **Week -1:** Transition support and clarify final questions
- **Day 0:** Close account and revoke access
- **Day +30:** Conduct post-engagement support review

Following offboarding, we will return all client data in agreed formats. For example, CSV, JSON or SQL. For a clear audit trail, we apply a 'right to audit deletion' process and provide certified data deletion within 30 days of contract end.

Data extraction

Client can request data back through the following methods:

- Making a formal request by email to dataprotection@technogise.com
- Directly using project repositories and documentation portals
- Through automated export, which is available for most systems

Data formats

The data formats that we provide are:

- **Standard formats:** CSV, JSON, XML, SQL
- **Documentation:** PDF, Markdown, HTML, Microsoft Word
- **Code repositories:** Git bundles, ZIP archives
- **Databases:** SQL dumps, native backups
- Custom formats are also available on request

3.3 Data

3.3.1 Data importing and exporting

Data import capabilities

Our service supports flexible data import from multiple sources:

- **Modern integrations:** RESTful APIs, GraphQL, OAuth 2.0, OpenID Connect
- **Legacy systems:** SOAP web services, file-based transfers, database-level integration
- **Standard protocols:** Following open standards including OpenAPI specifications

Data export and retrieval

Clients can request data back through multiple channels:

- **Formal request:** Email to dataprotection@technogise.com
- **Self-service:** Direct access through project repositories and documentation portals
- **Automated export:** Available for most systems

We provide data in standard, widely supported formats:

- **Structured data:** CSV, JSON, XML, SQL
- **Documentation:** PDF, Markdown, HTML, Word
- **Code repositories:** Git bundles, ZIP archives
- **Databases:** SQL dumps, native backups
- **Custom formats:** Available on request

Data deletion and security

At contract end or upon request:

- All client data returned in agreed formats
- Secure deletion completed within 30 days
- Deletion certificate provided for compliance
- Complete audit trail maintained
- Right to audit deletion process available

Avoiding vendor lock-in

Our approach prevents dependency through:

- **Open standards focus:** No proprietary formats or tools required
- **Knowledge transfer:** Client teams gain full capability to maintain solutions independently
- **Interoperability:** Standard APIs and connectors for major platforms such as AWS, Azure, GCP and Kubernetes
- **Portable architectures:** Solutions designed for platform independence where appropriate

3.3.2 Analytics

Performance monitoring and metrics

We deliver comprehensive performance monitoring aligned with ISO 9001 quality management standards. Our analytics framework provides clear visibility into service delivery and system performance.

Standard metrics tracked:

- **Incident response times:** P1 (2 hours), P2 (4 hours), P3 (8 hours), P4 (24 hours)
- **System availability:** 99.9% uptime for production systems
- **Deployment success rate:** >95% across all releases
- **Mean time to resolution:** P1 (4 hours), P2 (8 hours), P3 (24 hours)
- **Migration progress:** Component completion, risk mitigation status
- **Team velocity:** Sprint delivery metrics, knowledge transfer effectiveness

Analytics tools and platforms

We implement industry-standard monitoring and reporting:

- **Real-time dashboards:** Grafana and Prometheus for live system metrics
- **CI/CD analytics:** Pipeline performance, build success rates, deployment frequency
- **Service management:** Jira Service Desk for ticket tracking and SLA compliance
- **Application performance:** Custom monitoring tailored to client systems

Reporting and business intelligence

All analytics data is available in open, accessible formats:

- **Standard exports:** CSV, JSON, XML for integration with existing BI tools
- **API access:** RESTful endpoints for automated data extraction
- **Custom reports:** Tailored dashboards and reports aligned with client KPIs
- **Scheduled reporting:** Regular performance summaries delivered to stakeholders

Customisation for client needs

We adapt our analytics approach based on:

- Specific KPIs relevant to your organisation
- Integration with existing reporting tools such as Power BI and Tableau
- Regulatory or compliance reporting requirements
- Stakeholder-specific views (technical, executive, operational)

3.3.3 Independence of resource

Client resource isolation

Each client engagement operates in dedicated, isolated environments to prevent cross-client interference and ensure data security:

- **Separate infrastructure:** Dedicated cloud environments per client (AWS VPCs, Azure Resource Groups, GCP Projects)
- **Isolated data storage:** Client data segregated with no sharing between engagements
- **Independent access controls:** Role-based access specific to each client project
- **Separate CI/CD pipelines:** Dedicated deployment infrastructure preventing cross-contamination

Architectural isolation

Our microservices and containerisation approach provide inherent resource independence:

- **Container isolation:** Docker containers with resource limits (CPU, memory, storage)
- **Orchestration boundaries:** Kubernetes namespaces ensuring workload separation
- **Network segmentation:** Isolated networks prevent inter-client traffic
- **Multi-tenancy support:** Where shared infrastructure is used, strict logical separation is enforced

Performance independence

Client workloads remain unaffected by other activities:

- **Auto-scaling:** Automatic resource allocation based on individual client demand
- **Load balancing:** Intelligent traffic distribution, preventing performance degradation
- **Resource quotas:** Guaranteed minimum resources per client environment
- **Performance monitoring:** Real-time tracking ensures no client impacts another

Service resilience

Even under high demand, service stability is maintained through:

- **Continuous monitoring:** Proactive detection of resource contention
- **Automated failover:** Redundancy across availability zones
- **Guaranteed SLAs:** 99.9% uptime, >95% deployment success, 2-hour P1 response times
- **Capacity planning:** Regular assessment ensures adequate resources for all clients

3.4 Backup, restore & disaster recovery

3.3.1 Overview and governance

Ensuring business continuity, we implement the following measures:

- A formal Business Continuity and Disaster Recovery plan
- Multi-region deployment capabilities
- Automated failover procedures
- Quarterly Disaster Recovery testing
- Dedicated Crisis Management Team with defined escalation procedures
- Alternative working arrangements for Consultant availability
- Documented runbooks for all critical procedures

3.3.2 Backup and data protection

For GDPR and Data Protection Act compliance, we only process necessary data and build privacy by design into all our solutions. For example, to identify and mitigate risks early, we will:

- Confirm Data Processing Agreements (DPAs) for all parties
- Conduct regular Data Protection Impact Assessments (DPIAs)

To manage data responsibly, we implement clear data retention policies with defined deletion schedules. Our robust subject access request procedures ensure individuals can easily exercise their data rights. For timely and transparent communication in the event of an incident, we have a breach notification process and will provide a report within 72 hours.

We back up data at the following frequencies, in addition to conducting weekly full backups with monthly archives:

Data type	Frequency
Critical systems	Continuous replication
Application data	Hourly snapshots
Project artifacts	Daily

We store data at the following locations:

- **Primary storage:** UK data centres (London and Manchester)
- **Backup storage:** UK-based cloud regions (AWS eu-west-2 and Azure UK South)

3.3.3 Disaster recovery and restoration

Ensuring we are prepared in the event of disruption, our Disaster Recovery Plan sets out recovery priorities and escalation procedures. In the event of a disaster, we will restore services within the following Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO):

- **RPO:** Maximum 1 hour for critical systems and 4 hours for standard systems
- **RTO:** Maximum 2 hours for critical systems and 8 hours for standard systems
- Custom Service Level Agreements (SLAs) are also available based on specific requirements

Ensuring business continuity, we implement the following measures:

- Multi-region deployment capabilities
- Automated failover procedures
- Quarterly disaster recovery testing
- Dedicated Crisis Management Team with defined escalation procedures
- Alternative working arrangements for Consultant availability
- Documented runbooks for all critical procedures

Hard copy and physical records

As a cloud services provider, we primarily focus on digital backups. For limited scenarios where hard copy or physical records may exist, such as signed contracts or receipts, we apply appropriate technical and organisational measures. These include:

- Securely storing physical records in a locked cabinet or secure room with controlled access
- Maintaining a register to log location, custody and access history
- Limiting handling of backups to authorised personnel
- Applying a documented retention schedule, consistent with digital data retention
- Digitising physical records and storing encrypted digital copies in the cloud

Continuous improvement and assurance

In line with our Business Continuity and Disaster Recovery plan, we will conduct a formal review following a live incident. Maintaining full compliance with G-Cloud 15 Call-Off Terms and supporting continuous improvement, we will integrate lessons learned into our processes and procedures.

3.5 Service management details

3.5.1 Service levels and availability

The following Service Level Agreements (SLAs) define the standards that apply to our service under the G-Cloud 15 framework. As part of our service management reporting and continuous improvement approach, we regularly monitor these metrics to maintain standards in line with the contract.

SLA metric	Target	How we measure this
Response times	P1 – Critical (2 hours) P2 – High (4 hours) P3 – Medium (8 hours) P4 – Low (24 hours)	Time from incident/request logged in ticketing system (Jira Service Desk) to first substantive response from technical team member. Measured via: • Jira Service Desk automated timestamps • SLA clock starts: ticket creation • SLA clock stops: first engineer response (not auto-acknowledgement) • - Monthly reporting: % of tickets meeting target by priority
Availability	99.9% for production systems	For production systems under our management: uptime monitoring via Grafana/Prometheus with 5-minute interval checks. Measured via: • Synthetic monitoring (health check endpoints) • Calculation: (Total minutes Downtime minutes) / Total minutes × 100 • Excludes: planned maintenance windows, client-side issues • Monthly reporting: actual uptime % vs 99.9% target
Deployment success rate	>95%	Percentage of deployments to production that complete successfully without rollback or critical defects within 24 hours. Measured via:

		• CI/CD pipeline metrics (Jenkins/GitLab/Azure DevOps) • Success criteria: deployment completes, post-deployment tests pass, • No rollback required • Monthly reporting: successful deployments / total deployments × 100 • Target: >95% success rate
Mean time to resolution	P1 - 4 hours P2 - 8 hours P3 - 24 hours	Average time from incident logged to incident resolved and closed, by priority level. Measured via: • Jira Service Desk ticket lifecycle tracking • Clock starts: ticket creation • Clock stops: ticket marked resolved and verified • Excludes: time waiting for client input/approval • Monthly reporting: average resolution time by priority (P1-P4)

3.5.2 Support details

You can contact us for support on the following channels:

Support channels	• Email: support@technogise.com • Jira service desk ticketing system • Phone support (P1 and P2 issues)
Support hours	Between 9am and 6pm UK time, with extended hours available. For critical systems, we also offer on-call support.
Support accessibility	We provide multiple support channels to accommodate different needs, defined above. Providing flexibility, we can provide documentation, guides and knowledge base articles in accessible formats. For example, audio or large print.
Response times	Support is available within the following response times: **P1 – Critical (2 hours)** • Complete service outage affecting all users • Data loss or corruption in production environments • Security breach or suspected breach • Critical compliance violations

	• Resolution Target: 4 hours • Availability: 24/7 on-call support for P1 issues • Escalation: Direct to Technical Lead and Delivery Manager **P2 – High (4 hours)** • Major feature failure affecting significant user subset • Performance degradation impacting business operations • Workaround required but service partially available • Non-critical security concerns • Resolution Target: 8 hours • Availability: UK business hours (9am-6pm) with extended hours available • Escalation: Technical Lead within 2 hours if unresolved **P3 – Medium (8 hours)** • Minor feature issues affecting limited users • Questions about system functionality • Non-urgent configuration changes • Documentation requests • Resolution Target: 24 hours • Availability: UK business hours • Escalation: Standard escalation path **P4 – Low (24 hours)** • Feature requests • General inquiries • Enhancement discussions • Scheduled maintenance coordination • Resolution Target: 48-72 hours • Availability: UK business hours • Escalation: As needed
	The standard support levels we provide are: **L3 Support (Application/Platform Support):** Expert-level technical support provided by our senior engineers and architects who possess deep knowledge of the specific application architecture, codebase, and infrastructure, handling complex troubleshooting, root cause analysis, performance optimization, and escalated issues requiring code-level investigation or architectural changes. **L4 Support (Development & Engineering Support):** Advanced engineering support delivered by our core development team with direct access to source code and system design, responsible for resolving critical bugs, implementing emergency fixes, conducting deep-dive investigations into systemic issues, and providing code patches or architectural modifications for complex technical challenges beyond L3 scope.

	The costs for support are: • Consultant: £301/day • Senior Consultant: £352/day • Lead Consultant: £416/day • Principal Consultant: £608/day Other support levels are available upon request.
Support for third parties	No
AI/chatbots	No
Service management	**Named account management** Providing continuity, we assign a dedicated Account Manager and Technical Lead for all engagements from day 1. For strategic guidance, support and advocacy for strategic accounts, we will provide an Executive Sponsor. Supporting service quality, we conduct monthly governance meetings and quarterly business reviews. **Escalation process** At the start of service delivery, we will communicate escalation roles and responsibilities by providing you with a clear escalation matrix. In the unlikely event that an issue arises, we will categorise and escalate issues to the following individuals with our team: • Level 1: Technical Lead (immediate) • Level 2: Delivery Manager (within 2 hours) • Level 3: Account Director (within 4 hours) • Level 4: CEO (within 24 hours)

3.6 Training

Ensuring that your team fully adopts and maintains our cloud services, we include training and knowledge transfer as a core part of each project. Meeting your exact requirements, we tailor training programmes to your systems, workflows and users.

3.6.1 Formats

For close collaboration and seamless integration, our Consultants work alongside client teams using an embedded delivery model. To foster transparency and shared understanding, we facilitate regular workshops on architecture decisions, sprint planning and retrospectives.

We promote knowledge transfer through hands-on pair programming, while regular demos and feedback sessions keep stakeholders engaged throughout the process. To enable effective face-to-face collaboration, we offer co-location options for critical project phases.

Supporting ongoing communication, we also use shared documentation tools, such as collaborative wikis and knowledge bases. Finally, we encourage joint problem-solving through architecture review boards and technical decision forums.

Ensuring client understanding, we offer training in a range of learning formats. Examples of training we provide include:

- On-site workshops on topics such as architecture, DevOps and cloud technologies. In addition, we will support you to comply with G-Cloud 15-related central government policies, including the Cloud First Policy and Technology Code of Practice. We support clients in meeting these standards through open standards adoption, cloud-native architecture, accessibility-first design, and transparent knowledge transfer
- Virtual training using live online sessions on Teams or Zoom
- "Train the trainer" sessions, enabling client teams to cascade knowledge
- Hosting lunch and learn sessions to promote Informal knowledge sharing
- 'Pair programming' to support learning through doing
- Hands-on labs, providing practical exercises in our client's environment

3.6.2 Materials

Delivering comprehensive support, we provide a range of training materials tailored to client needs. For example:

- Comprehensive documentation such as architecture decisions, runbooks and playbooks
- Code examples with explanations on how to implement them
- Best practice guides, tailored to client contexts
- Video tutorials and recorded training sessions
- A dedicated knowledge base and wiki setup using Confluence software
- Handover packs with complete transition documentation

3.6.3 Training pricing

Providing value to our clients, we include knowledge transfer at no cost during delivery, documentation and pair programming.

Dedicated training workshops, certification preparation and specialised courses are charged at £1,500 per day. For clients with high-volume training needs, we offer training credits and bundle options.

3.7 Service pricing

We offer a range of pricing models to suit client requirements under G-Cloud 15. Full pricing details are available in the separate Pricing Document.

Pricing models available

Pricing model	Purpose
Time and materials	Flexible engagement for evolving requirements
Fixed price	For well-defined discovery and assessment phases
Outcome-based	Tied to specific migration milestones
Retainer	For ongoing support and optimisation
Blended rate model	Simplified billing across all Consultant levels

Rates

Our typical day rates are defined below:

Role	Rate
Consultant	£301/day
Senior Consultant	£352/day
Lead Consultant	£416/day
Principal Consultant	£608/day
Blended Rate	£352/day (recommended for most engagements)

Pricing Tiers

We offer 3 pricing tiers: Discovery, Pilot and Full Migration, each with varying levels of features and support, along with ongoing priced support.

Discovery package (£25,000-£50,000)

- 4-6 week assessment
- Current state analysis
- Migration roadmap
- Risk assessment
- Budget estimation

Pilot implementation (£75,000-£150,000)

- 8-12 week pilot
- First component migration
- CI/CD pipeline setup
- Team training

Full migration (£150,000+)

- Complete system transformation
- Based on system complexity
- Includes all phases

Ongoing support (£10,000-£25,000/month)

- Optimisation services
- Issue resolution
- Continuous improvement

Additional charges

Additional charges may apply for the following:

- **On-site delivery:** Travel and accommodation at cost
- **Specialised training:** £1,500/day for dedicated training sessions
- **Emergency support:** 1.5x standard rates for critical issues
- **Additional cloud resources:** Pass-through at cost
- **Third-party tool licenses:** At cost if required

SFIA rate card

Our complete SFIA-aligned rate card is available upon request. The rate card maps our roles to SFIA levels 3-7 across relevant skills, including:

- ARCH (Solution Architecture)
- PROG (Programming/Software Development)
- TEST (Testing)
- SCMG (Service Capacity Management)
- RLMT (Release Management)

3.8 Invoicing process

Invoicing schedule
Our standard invoicing cycle is monthly for Time and Materials (T&M) engagements, whilst fixed-price projects are based on milestones. For clients with retainer agreements, we offer quarterly invoicing options.

Payment terms
Our standard payment terms are 30 days. Our preferred payment methods are:

- BACS
- Bank transfer

Providing flexibility, we also support PO-backed invoicing. Additionally, we offer the following options for client self-billing portals:

- Integration with Government Procurement Cards (GPC)
- Compatible with major Peer-to-Peer (P2P) systems
- Self-billing agreements
- Electronic invoicing via PEPPOL network

3.9 Termination terms

Termination is governed by the Crown Commercial Service G-Cloud 15 Call-Off Terms and Conditions. Buyers may terminate the contract in accordance with these terms by providing written notice. Technogise may terminate only in cases of material breach or non-payment. Upon termination, all data will be handled in line with our offboarding and data-deletion process described in Section 3.2.2.

4 Security and data governance

4.1 Data protection and encryption

To protect data in transit and within supplier networks and ensure GDPR and Data Protection Act compliance, we only process necessary data and build privacy by design into all our solutions. As standard practice, we follow the Government Service Standard 'Secure By Design' Principles. This means that to effectively protect your data, we will:

- Create responsibility for cyber security risk for our service and throughout its lifecycle
- Consider cyber security and at our senior leadership level in accordance with the project risk
- Perform security due diligence by continually assessing platforms, software and code for security vulnerabilities
- Adopt a risk-driven approach that can evolve to emerging threats
- Design usable security controls that minimise friction for users by making security protocols fit for purpose and easy to understand
- Integrating appropriate security logging, monitoring, alerting and responding capabilities to detect, respond to and recover from incidents effectively
- Design flexible architectures that respond quickly to evolving cyber threats
- Embed continuous assurance processes to mitigate risks at all stages

To identify and mitigate risks early, we will:

- Confirm Data Processing Agreements (DPAs) for all parties
- Conduct regular Data Protection Impact Assessments (DPIAs)

Managing data responsibly, we implement clear data retention policies with defined deletion schedules. Our robust subject access request procedures ensure individuals can easily exercise their data rights. For timely and transparent communication in the event of an incident, we have a breach notification process and will provide a report within 72 hours.

4.2 Data at rest, storage locations and physical security

We will protect stored data through documented asset control, appropriate technical and physical safeguards and clear supplier arrangements. Addressing privacy and data-protection risks when choosing storage locations and technical safeguards, we apply "privacy by design" principles when determining storage architecture and configurations.

Where data is stored and who manages it

We maintain an information-asset register that records what data we hold, where it is stored, the type of storage media and the named owner responsible for that data. We keep this register current through lifecycle events (provisioning, migration, decommission).

Encryption and technical controls

Consistent with ICO guidance, we protect data at rest containing personal or sensitive information by appropriate technical controls. For example, encryption at rest, access controls and logging.

Hosting location

We store and process data securely in UK data centres (London and Manchester). Our cloud regions are AWS eu-west-2 (London), Azure UK South. We protect data with our UK-based infrastructure and do not conduct offshore processing without explicit consent.

Data-centre certifications and physical controls

For cloud or co-location services, we will use providers that demonstrate robust security controls such as ISO 27001 certification or equivalent. Where physical (on-premise or co-located) infrastructure is used, we will require appropriate physical controls such as access control and environmental monitoring. Supporting audit and incident investigation, we log and retain access to data stores.

Sub-processors

We use the following GDPR-compliant sub-processors:

- **Cloud providers:** AWS (UK), Microsoft Azure (UK), Google Cloud (UK)
- **Collaboration tools:** Microsoft (UK/EU), Atlassian (EU)
- **Development tools:** GitHub (EU), GitLab (EU)

4.3 Data sanitisation and disposal

For a clear audit trail, we apply a 'right to audit deletion' process and provide certified data deletion within 30 days of contract end. We will securely erase and dispose of data and hardware, with documented proof of disposal where appropriate. Our process is detailed below.

Sanitisation

We retire all storage media and devices through a documented process. This involves:

1. Identifying the media
2. Classifying data sensitivity
3. Selecting an appropriate sanitisation method
4. Executing sanitisation
5. Recording results in an asset register

Methods and verification

Where media is to be reused, we will use approved secure-erase processes, such as secure overwrite or cryptographic erasure and verify successful sanitisation before reuse. Where media is to be destroyed, we will use appropriate physical destruction methods for the media type and sensitivity. For audit purposes, we will record the serial numbers and destruction evidence.

Third-party disposal partners

Where we use external disposal or recycling suppliers, contracts will require demonstrable secure-disposal capability and chain-of-custody records. Where feasible, we will obtain a certificate of destruction or sanitisation from the supplier and retain this evidence against the asset record.

Retention and deletion policy

We maintain and apply a retention schedule that specifies how long categories of data are kept and the sanitisation or deletion action when retention ends. To provide continuous oversight, we periodically review retention schedules and apply them consistently to live data and backups.

4.4 Security testing and assurance

To ensure our systems remain protected against emerging threats, we operate a regular programme of security testing. This is consistent with the UK Government's Secure by Design guidance, which highlights the need for ongoing vulnerability discovery and testing. Our approach includes:

Penetration testing

We schedule external penetration tests at least annually for standard-risk services, and quarterly for high-risk services (those processing sensitive data or critical operations). We also conduct penetration tests after major system changes, significant architectural updates, or before production deployment of new capabilities. All testing is conducted by CREST-certified or equivalent qualified security professionals.

Vulnerability scanning

Vulnerability scanning runs continuously on production environments via automated tooling (AWS Inspector, Azure Defender, Snyk). Weekly comprehensive scans cover all infrastructure and application layers. All findings are automatically logged with severity ratings. Remediation SLAs: Critical vulnerabilities within 48 hours, High within 7 days, Medium within 30 days. All issues tracked in risk register with status reporting to senior stakeholders.

Reporting and follow-up

Providing a prompt resolution, we will provide all test results to senior stakeholders, track them in a risk register and retest after remediation.

4.5 Incident and protective monitoring management

We maintain strong monitoring and incident-response capabilities, aligned with UK Government expectations to “detect and respond” to security issues. Our approach includes:

24/7 monitoring

Enabling us to rapidly detect suspicious activity, we continuously monitor security logs and events through automated security monitoring and alerting infrastructure. Our security monitoring includes real-time threat detection, automated anomaly alerts, and 24/7 on-call security response capabilities with defined escalation procedures for critical security incidents.

Incident handling processes

Ensuring timely reporting to internal leaders and external bodies, we provide clear escalation routes and notification timelines. For clarity, we classify incidents by severity and manage them through a structured process covering detection, containment, eradication and recovery.

Post-incident learning

For continuous improvement, we conduct a structured review after all major incidents and critical security events to identify root causes and implement preventive controls. For consistency and traceability, our process is aligned with ISO 27035 incident management principles. Lower-severity incidents are reviewed through periodic trend analysis to identify systemic issues.

4.6 Configuration and change management

Protecting service stability and security, we manage changes in a controlled, auditable way:

- **ITIL-aligned change control:** Following documented processes covering planning, impact assessment, testing, approval and deployment. Changes are categorized (standard/normal/emergency) with appropriate approval workflows and rollback procedures
- **Version control and testing:** All code and configuration changes are version-controlled (Git), peer-reviewed, and tested in non-production environments before release. Automated testing includes unit, integration, and security tests. Rollback procedures maintained for rapid recovery
- **Change Advisory governance:** Significant or higher-risk changes are reviewed through formal change advisory processes. For client systems, we participate in client governance structures (CAB, architecture review boards). Our internal technical review board assesses all changes for technical quality and risk before submission to client approval processes
- **Audit and traceability:** All changes tracked with full audit trail including rationale, approvals, test results, and outcomes. Change records maintained in compliance with client retention requirements

4.7 Information security management and certifications

Providing clear responsibility, Vivek Singh is our Information Security Manager. They oversee all security governance, risk management and compliance activities. We operate a formal information-security governance framework and hold recognised certifications. The relevant security certifications our team members hold include AWS Security and Azure Security Engineer. Supporting data security, we are Cyber Essentials ready and will attain ISO 27001 information security management systems (ISMS) certification by Q4 2026.

4.8 Secure development and cryptography

Addressing vulnerabilities early, we build security into every stage of the development lifecycle. Our approach includes:

- **Secure development lifecycle (SDLC):** Aligned with the Secure by Design guidance on vulnerability discovery, throughout development, we apply:
  - **Code reviews**
  - **Automated security testing (SAST/DAST)**
  - **Dependency scanning**
  - **Peer reviews**
- **Open Worldwide Application Security Project (OWASP) Top 10:** As recommended in the government guidance, we develop and test web applications against the OWASP Top 10, enabling us to produce more secure code
- **Cryptographic controls:** In accordance with the guidance from the Information Commissioner's Office (ICO), under UK GDPR, we will use appropriate cryptographic measures where personal or sensitive data is processed or stored. For example, by using encryption in transit and at rest

4.9 Identity and access management

Protecting both user and administrator access, we implement strong identity and access-control measures. These include multi-factor authentication for administrator accounts and users where appropriate. Additionally, we implement role-based access control (RBAC), granting access based on the job role and the principle of least privilege.

5 Supplier information

5.1 About us

Founded in November 2015, Technogise is a bespoke software development company.

We specialise in solving complex technical challenges for global clients across financial services, gaming, e-commerce, retail, healthcare and education sectors.

With delivery centres in Pune, Bangalore and London, our key project leadership spans India, Europe and the UK.

Our team of 100 Consultants has successfully delivered transformative solutions for organisations ranging from startups to large-scale enterprises operating in more than 25 countries.

At Technogise, our mission is simple.

We get it, we get it done, we get it done right.

To deliver lasting business value, we embed the following core values when partnering with forward-thinking organisations to create cutting-edge digital products and services:

1. **Client success:** Treating client challenges as our own
2. **Technical excellence:** Using clean code, applying SOLID design principles and test-driven development
3. **Sharing knowledge:** Upskilling and empowering client teams
4. **Innovation:** Embracing emerging technologies responsibly, such as AI
5. **Integrity:** Fostering transparent, honest partnerships

As regulated environmental specialists with proven migration expertise, we have successfully modernised billion-pound platforms with **zero downtime**. Delivering rapid results for our clients, we provide demonstrable value in under 12 weeks. With a global reach, our international team bring experience with both UK and EU clients. Our blended rate model drives value by providing clients with premium expertise at competitive prices.

5.2 Relevant experience and testimonials

Case study – Peak XV (Venture capital sector)

Peak XV required cloud support services including legacy ASP.NET migration to modernise their architecture and implement AI-augmented development. As the client had a classic ASP platform from the early 2000s, this had been difficult for them to maintain. Additionally, they lacked documentation across hundreds of files, with limited team bandwidth internally to support modernisation.

Providing flexibility, we delivered this contract using a hybrid model, combining remote delivery with on-site workshops in London. To safely migrate their systems, we implemented Strangler Fig pattern methodology using a phased rollout and toggle features. To accelerate code conversion, we used AI tools such as ChatGPT and Gemini. We reduced migration phase time for Peak XV by up to 70%, improved system performance by 40% and maintained zero downtime throughout the transition.

Case study – Universal Education (Education sector)

Universal Education required migration to their EdTech platform (Ether app), a school Enterprise Resourcing Planning (ERP) system update and an administration portal to enable multi-location management. With development centres in Pune and Mumbai, Universal Education required deployment across 5 school locations in India.

A key challenge that we addressed on this project was that there was no unified platform for school operations due to a lack of modern communication tools. As a result, the client was conducting extensive manual processes for admissions and assessments. To address this need, we built a comprehensive mobile app for parents and students. Key features included automated admission workflows, attendance tracking and integrated payment systems. Reducing manual processing time by 90%, we transitioned the client to 100% paperless operations. To date, the app has 10,000 + active users.

Case study – Entain (Sports sector)

Entain required key improvements to their platform reliability, optimised performance and an automated infrastructure. The client's platform instability was affecting their user experience. Additionally, manual deployment processes were causing delays, compounded by lack of real-time monitoring.

Supporting operations in the UK, Gibraltar and Austria, we delivered this project 100% remotely. To facilitate real-time monitoring, we built comprehensive monitoring capabilities with Grafana. Addressing delays and instability, we implemented an automated deployment pipeline and optimised Entain's database performance. Delivering tangible results, we improved platform response times by 35% and reduced deployment time by 60%. Optimising the client's performance and preventing bottlenecks, we maintained 99.9% uptime throughout the project.

Testimonials

"Technogise transformed our legacy platform into a modern, scalable architecture without a minute of downtime. Their expertise in financial services compliance and commitment to knowledge transfer made them an invaluable partner." ***- CTO, Leading Fintech***

"The team's approach to incremental migration using strangler fig pattern allowed us to modernise while maintaining full operations. The 28% improvement in deployment times exceeded our expectations." ***- Head of Technology, Gaming Platform***

"Their blend of technical excellence and knowledge sharing has built lasting capability in our teams. The value delivered far exceeded the investment." ***- Digital Transformation Director, Enterprise Client***

5.3 How to buy

Technogise's services can be procured directly through the Crown Commercial Service (CCS) G-Cloud 15 Digital Marketplace.

Buyers can search for Technogise on the Digital Marketplace and select the required service listing.

Once selected, the buyer and Technogise will:

1. Agree a Statement of Work (SOW) detailing scope, deliverables, timescales and pricing
2. Raise a Call-Off Contract under the G-Cloud framework terms
3. Issue a Purchase Order (PO) to confirm commencement

Ensuring transparency and compliance with public-sector procurement regulations, all engagements are delivered in line with G-Cloud framework conditions.

Enquiries or pre-contract discussions can be arranged through our central contact point:

- Ryan Bayly at ryan@technogise.com
- +44 7880 557 177