Adappt

Adappt – Lot 3
Cloud Support Service

General Service Definition (G-Cloud 15)

Citation ISO Certification — Information security management — ISO 27001: 2013 — REGISTERED

Citation ISO Certification — Quality management — ISO 9001: 2015 — REGISTERED

CYBER ESSENTIALS

Table of Contents

Adappt – Lot 3 Cloud Support Service
General Service Definition (G-Cloud 15)

Working Hours: 09:00–17:30 UK time, Monday to Friday (excluding UK public holidays). Weekend or extended-hours support can be provided by prior agreement at additional cost.

Executive Summary

Adappt provides Lot 3 Cloud Support Services to help public sector and regulated organisations design, migrate, secure, operate, and improve cloud-based services. With over 15 years' experience, we support critical digital services across healthcare, regulatory bodies, and international organisations.

Our work spans the full cloud service lifecycle, from early assessment and planning through secure implementation, testing, assurance, enablement, and ongoing support. We have delivered cloud and data services for organisations including the World Health Organization (WHO) and the General Pharmaceutical Council (GPhC), where security, resilience, data protection, and auditability are essential.

Adappt's approach is engineering-led and evidence-driven. We focus on practical delivery, clear service boundaries, and strong handover so that buyer teams can operate and evolve their cloud services with confidence. This Service Definition provides a comprehensive baseline description of Adappt's Lot 3 Cloud Support Services and is intended to be used alongside Order Forms or Statements of Work that define buyer-specific requirements.

1. Purpose of this document

This Service Definition describes Adappt's Lot 3 Cloud Support Services for buyers seeking support, delivery and assurance across public cloud environments (primarily AWS and Azure, and where relevant Cloudflare). It is intended to be used as a general, reusable service definition across Adappt's Lot 3 offerings.

The document explains: what we deliver (service catalogue); how we deliver (methods, governance, quality and security); what buyers need to provide (dependencies and responsibilities); service boundaries (constraints and exclusions); and how support works (channels, hours, severity and escalation).

This Service Definition is written to support G-Cloud submission and procurement evaluation, and to be used as a baseline for Statements of Work / Order Forms.

2. About Adappt

Adappt is a UK-based technology consultancy with over 15 years' experience delivering complex digital, data, and cloud services for public sector, healthcare, and regulated organisations. We specialise in cloud engineering, security-led delivery, and operational assurance across AWS, Azure, and related cloud platforms.

Adappt has supported organisations including the World Health Organization (WHO), UK Home Office, Defra, FCDO, Security & Policing, General Pharmaceutical Council (GPhC), and other public and regulated bodies to design, build, migrate, and operate cloud-based services that are secure, resilient, and auditable. Our work commonly supports services operating under heightened regulatory, data protection, and availability requirements.

We combine hands-on engineering with strong governance and assurance practices. This means we do not only design solutions, but work alongside buyer teams to implement, validate, and hand over services in a way that supports long-term operation and compliance. Our teams are experienced in working within multi-supplier environments and established public sector delivery models.

Adappt's approach is pragmatic and outcome-focused. We prioritise reducing delivery risk, producing clear evidence for assurance, and enabling buyer teams to operate and evolve their cloud services with confidence once our engagement concludes.

3. Service overview

Adappt's Lot 3 Cloud Support Services are delivered as professional services that can include assessments and planning, implementation and change, quality and assurance, enablement, and ongoing support.

Services are typically delivered remotely. Onsite delivery can be provided by prior agreement.

3.1 What "Cloud Support" means in this definition

Within Lot 3, "Cloud Support" covers work that helps a buyer design, build, improve, secure, migrate, test, or support cloud-based services. Unless explicitly stated in an Order Form, Adappt does not provide 24/7 managed operations, a managed security operations centre (SOC), or long-term platform "run" services as an MSP.

Where extended hours, weekend support, or more operational coverage is required, this can be agreed and priced separately.

4. Service catalogue (Lot 3)

Adappt provides the following service lines under Lot 3. Each service can be procured independently or combined.

4.1 Secure Cloud Migration and Legacy Modernisation (AWS/Azure)

We plan and deliver secure migration and modernisation of services from legacy or on-premise environments to AWS or Azure. This includes readiness assessment, target architecture design, migration sequencing, cutover planning, secure configuration, and operational handover. Modernisation can include re-platforming, refactoring, and the creation of cloud-native operating patterns.

Typical outcomes: migration roadmap and sequencing plan; secure landing zone and baseline controls; migrated applications/data (where in scope); validated cutover and handover documentation.

4.2 DevSecOps and Secure CI/CD Acceleration (AWS/Azure)

We design and implement secure delivery pipelines and platform automation so teams can deploy changes safely and repeatedly. This includes CI/CD design, infrastructure as code (IaC), security scanning and policy enforcement, automated testing integration, secrets management, and release governance.

Typical outcomes: secure, repeatable CI/CD pipelines; IaC patterns and environment standardisation; integrated testing and security controls; documented operating model and enablement.

4.3 Platform Engineering and SRE for Mission-Critical Services

We build and improve cloud platforms to support reliability, availability, and performance for mission-critical services. This includes observability, capacity planning, resilience design, incident readiness, and reliability improvements aligned to SRE principles.

Typical outcomes: platform foundations and operational patterns; monitoring/alerting and incident readiness; capacity and performance baselines; validated resilience and handover artefacts.

4.4 Secure AI Adoption

We enable secure adoption of AI capabilities in cloud environments. This includes planning and implementing secure AI environments, controls for identity and data protection, governance guardrails, monitoring and operational readiness. Work can support AI-enabled services while maintaining compliance and risk management.

Typical outcomes: secure AI workload architecture and controls; governance and access guardrails; validated deployments and documentation; enablement for safe operation.

4.5 Cyber Security Assurance for Cloud Services (AWS/Azure/Cloudflare)

We provide assurance services to assess and strengthen cloud security posture. This includes architecture review, risk assessment, identity and configuration review, monitoring controls assessment, and prioritised remediation guidance. Where agreed, we can support implementing remediation actions.

Typical outcomes: security posture assessment and findings; prioritised remediation plan; evidence packs for assurance and audit; incident readiness recommendations.

4.6 Service-to-outcomes mapping (summary)

- Secure Cloud Migration and Legacy Modernisation: safer transition to cloud, reduced migration risk, improved maintainability
- DevSecOps and Secure CI/CD Acceleration: faster, safer delivery of change with embedded security and quality
- Platform Engineering and SRE: improved reliability, performance, and resilience of mission-critical services
- Secure AI Adoption: controlled adoption of AI capabilities with governance and risk management
- Cyber Security Assurance: improved security posture, compliance confidence, and audit readiness

5. Standard service components (used across service lines)

Buyers commonly procure a combination of the following components, which apply across the service catalogue.

5.1 Cloud migration planning

- Discovery and readiness assessment
- Architecture options analysis
- Dependency and risk analysis
- Migration sequencing and roadmap
- Cutover and rollback planning
- Governance, compliance and operational requirements definition

5.2 Set up and migration

- Environment build and configuration (including landing zones)
- Identity, network and baseline security configuration
- Infrastructure as code implementation
- Controlled migration and validation
- Cutover support and operational readiness
- Documentation, runbooks and knowledge transfer

5.3 Security services

- Security strategy and design
- Risk assessment and threat modelling
- Secure configuration baselines
- Logging, monitoring and incident readiness
- Audit/assurance evidence support
- Remediation planning and (where agreed) implementation support

5.4 Quality assurance and performance testing

- Test strategy and assurance planning
- Configuration, integration and infrastructure testing
- Performance, load and capacity testing
- Resilience/failure scenario testing (where agreed)
- Evidence collection and reporting

5.5 Training and enablement

- Role-based training and walkthroughs
- Troubleshooting and optimisation training
- Operational process and incident readiness training
- Documentation and knowledge transfer

5.6 Ongoing support

- Email and ticketing support
- Severity-based triage
- Investigation and troubleshooting
- Operational guidance and reporting
- Post-incident reviews and recommendations

5.7 FinOps (where in scope)

Where agreed, we support cloud cost visibility and governance, including tagging strategies, cost reporting, forecasting inputs, and optimisation recommendations aligned to delivery and operational needs.

6. Delivery approach

6.1 Principles

- Security by design: security and compliance embedded from the outset
- Reliability-focused: platforms and services designed for availability and supportability
- Automation-first: use of infrastructure as code and repeatable delivery patterns
- Evidence-led assurance: artefacts produced to support audit, assurance, and governance

- Knowledge transfer: enabling buyer teams to operate services independently

6.2 Typical phases

1. Discovery and mobilisation – confirm objectives, constraints, stakeholders, and success measures; confirm access, security approvals, and working arrangements; agree delivery plan, governance model, reporting cadence, and risks.

2. Assessment and design – architecture, security, and operational requirements; service roadmap, sequencing, and dependencies; assurance, testing, and acceptance planning.

3. Implementation and change – configuration, automation, migration, or remediation activities; continuous validation, peer review, and evidence capture; change control and stakeholder communication.

4. Validation and readiness – testing, performance validation, and security checks; operational readiness, runbooks, and support processes.

5. Support and transition – hypercare or short-term post-change support (where agreed); transition to buyer-led operation or ongoing support arrangements.

7. Roles and resourcing

Adappt provides appropriately skilled roles depending on scope, which may include Cloud Architect, Platform Engineer / SRE Engineer, DevSecOps Engineer, Security Consultant / Assurance Lead, QA / Performance Test Engineer, and Delivery Lead / Project Manager. A named technical lead or cloud support engineer can be provided where agreed.

8. Service management, support and escalation

8.1 Support channels

Support is provided via email and online ticketing.

8.2 Support hours

Standard support is delivered during Working Hours (09:00–17:30 UK). Weekend or extended hours support can be provided by prior agreement at additional cost, with response targets agreed in advance.

8.3 Severity and response targets

Requests are prioritised by severity. Indicative response targets (unless otherwise agreed):

- Critical: response within 4 working hours

- High: response within 1 working day
- Low/Normal: response within 2 working days

These targets apply during Working Hours.

8.4 Escalation

Where an incident or risk is significant, we escalate to the named buyer contact and Adappt technical lead. For critical incidents, we agree containment steps, evidence capture, communications, and remediation actions.

9. Governance, reporting and change control

9.1 Governance

We establish proportionate governance aligned to the size and criticality of the engagement. This typically includes a named Buyer Product Owner or Service Owner, an Adappt Delivery Lead responsible for coordination and quality, and agreed decision-making authority and escalation paths.

9.2 Reporting

We provide regular reporting appropriate to the engagement, which may include progress against milestones and deliverables, risks and dependencies, security and assurance findings, and actions and decisions. Reporting formats and cadence are agreed during mobilisation.

9.3 Change control

Changes to scope, assumptions, timelines or cost are managed through a lightweight change control process. All material changes require written agreement before implementation.

10. Security and assurance

Adappt aligns delivery to buyer security requirements and applicable standards. Typical controls and practices include least privilege and role-based access, secure configuration baselines, encryption in transit (TLS 1.2+) and at rest (where applicable), centralised logging and monitoring patterns, vulnerability management and remediation planning, and incident readiness and response planning. Where the buyer requires specific assurance artefacts, we agree these deliverables in advance.

11. Data handling

11.1 Buyer-controlled environments

Unless explicitly agreed otherwise, services are delivered within buyer-controlled cloud environments. The buyer remains responsible for cloud account/tenant ownership, connectivity, access approvals, licensing and subscriptions, and data classification decisions.

11.2 Access to buyer data

Adappt access to buyer environments and data is limited to what is required for delivery and support. Access is managed using least privilege and is time-bounded where practical.

11.3 Offboarding

At the end of an engagement we provide agreed handover artefacts. Where ongoing access has been granted, it should be removed by the buyer unless explicitly agreed otherwise.

12. Quality management

We use quality controls proportionate to scope, which may include peer review of designs and infrastructure code, documented acceptance criteria, structured testing and evidence collection, post-implementation validation, and retrospectives and lessons learned.

13. Service constraints and exclusions

Common constraints: services are primarily remote; onsite by agreement. Delivery timelines depend on timely buyer access to systems, environments, documentation and stakeholders. Migration or remediation work may require planned downtime or agreed change windows.

Common exclusions unless explicitly agreed: 24/7 managed operations or on-call cover; managed SOC/continuous security monitoring; end-user service desk or device support; ongoing testing services as a managed function; buyer licensing, connectivity or third-party costs.

14. Pricing and commercial model

Fees are provided on a time-and-materials or fixed-price basis depending on scope. Any extended hours or weekend support is priced separately. All pricing assumptions and inclusions are confirmed in the Order Form.

15. Deliverables

Deliverables are agreed per engagement and may include: architecture and design documentation; infrastructure as code and configuration artefacts; security findings, remediation plans, evidence packs; test plans, results and performance reports; runbooks, operating guides and handover documents; and training materials.

16. Handover and knowledge transfer

We provide handover as part of delivery, typically including documentation review sessions, walkthroughs of implemented configurations, operational readiness and support guidance, and training where in scope.

17. Buyer and Adappt responsibilities (RACI-style overview)

17.1 Adappt responsibilities

- Deliver services in line with the agreed scope and this Service Definition
- Provide suitably skilled resources
- Maintain delivery quality, security, and assurance
- Produce agreed documentation, evidence, and handover artefacts
- Escalate risks and issues in a timely manner

17.2 Buyer responsibilities

- Provide timely access to cloud environments, systems, and documentation
- Approve designs, changes, and deliverables
- Ensure appropriate internal governance and security approvals
- Manage cloud subscriptions, licensing, and third-party services
- Operate the service following handover unless otherwise agreed

18. Service options and tailoring

This Service Definition provides a common baseline for Lot 3 Cloud Support Services. Each Order Form or Statement of Work will specify selected service lines and components, deliverables and acceptance criteria, timeline and resourcing, support arrangements and response targets, pricing model and assumptions. Services can be combined and tailored to meet buyer needs while remaining within Lot 3 Cloud Support boundaries.

19. Why Adappt

- 15+ years' experience delivering complex digital, data, and cloud services
- Proven delivery in regulated environments, including healthcare and international organisations

- Engineering-led capability, not advisory-only consultancy
- Security and assurance expertise embedded throughout delivery
- Clear service boundaries that reduce procurement and delivery risk
- Evidence-driven outputs suitable for audit and governance
- Collaborative working style alongside buyer teams and other suppliers
- Practical outcomes that prioritise sustainable operation, not just implementation

20. Illustrative public sector use cases (anonymised)

The following examples illustrate how Adappt's Lot 3 Cloud Support Services are commonly used by public sector and regulated organisations:

- International health organisation: supporting a global health body to design and operate secure cloud platforms for data-intensive services, including architecture design, security assurance, and operational readiness aligned to international governance and data protection expectations.
- UK healthcare regulator: supporting a national regulator to modernise legacy systems and adopt cloud-native platforms, including secure migration planning, DevSecOps enablement, and evidence generation to support internal assurance and external audit.
- Public-facing digital service: improving the reliability and resilience of a mission-critical cloud service through platform engineering, observability, and incident readiness aligned to SRE principles.
- Security assurance engagement: assessing cloud security posture and providing prioritised remediation and evidence packs to support governance, accreditation, and audit activities.

These examples are indicative and reflect Adappt's experience delivering cloud support services in regulated and high-assurance environments.

21. Contact and next steps

Buyers can engage Adappt to discuss requirements, confirm scope, and agree the appropriate delivery model. We can provide sample deliverables, governance artefacts, assurance evidence, and anonymised examples on request.