Zanloop Ltd – G-Cloud 15 Lot 3 Cloud Support

Post-Quantum Cryptography Cloud Enablement Services
Company Number: 13327085

---

1. Executive Overview

The UK public sector depends on cryptography to ensure the confidentiality, integrity and resilience of essential national services. This spans:

• Citizen-facing digital platforms (taxation, benefits, justice, licensing)
• NHS and population-scale health and genomics data
• Police, border, defence and national security operations
• Local government operational systems and public safety environments
• Government-approved cloud and hybrid data architectures

Cryptography is everywhere in these systems — embedded into increasingly complex cloud services, outsourced supply chains and third-party Software-as-a-Service (SaaS) platforms. However, cryptographic implementation is often **poorly mapped**, **inconsistently configured**, and **not easily governed**.

Quantum Threat — The Urgency

Quantum computing progress introduces a generational cyber risk:

• **Classical cryptography will be broken** (RSA, ECC, ECDSA, ECDH)
• Adversaries are already **harvesting encrypted data** now to decrypt later
• Cloud supply-chains obscure where risk resides
• Long-retention public-sector data heightens exposure for decades
• Government assurance bodies require **cryptographic transparency**

The threat is not theoretical — it has become a live operational concern for:

• Government cyber and national security planning
• NHS patient-record retention requirements
• HM Treasury spend approval and accountability
• NCSC and Government Security Function oversight

Delaying transition increases:

• Future operational disruption
• Transformation cost and complexity
• National-scale systemic vulnerability
• Accountability and compliance risks

Zanloop's Purpose

Zanloop provides specialist cryptographic and cloud-security advisory services focused on:

• **Discovery** — mapping cryptography across cloud environments
• **Prioritisation** — quantified PQC readiness and risk exposure
• **Architecture** — controls to enforce PQ-secure future states
• **Enablement** — secure uplift under Buyer control
• **Governance** — continuous assurance and resilience oversight

We help organisations:

• Understand where cryptography actually is
• Control transition and avoid costly re-architecture later
• Demonstrate clear accountability to governance and audit
• Reduce risk of catastrophic crypto failure in future

Lot-3 Cloud Support Only

Zanloop does **not** operate live services.
We do **not** provide SOC, incident response, CHECK, or managed services.
The Buyer **always retains**:

• Control of production environments
• Responsibility for deployment decisions
• Ownership of operational monitoring and resilience

Cyber Essentials (or equivalent) can be obtained in line with framework requirements and buyer call-off conditions. Staff clearance will be obtained as required by call-offs, including BPSS/SC if needed. Support delivered during UK business hours (no 24×7 commitments).

Zanloop services support major public cloud platforms (AWS, Azure, GCP) and hybrid architectures.

---

2. Service Catalogue

Five standalone services (each independently procurable):

1. Post-Quantum Cryptography Cloud Encryption Discovery
2. Post-Quantum Cryptography Cryptographic Risk & PQ Readiness Assessment
3. Post-Quantum Cryptography Cryptographic Architecture & Controls Review
4. Post-Quantum Cryptography Migration Enablement: Cloud Cryptographic Uplift
5. Post-Quantum Cryptography Governance & Cloud Resilience Advisory

All services:

• Focus solely on **cloud support and enablement**
• Are **public-sector-aligned**
• Deliver **tangible artefacts** for governance and assurance
• Keep the Buyer in control at all times

Service 1 — Post-Quantum Cryptography Cloud Encryption Discovery

Full cryptographic visibility and initial PQ readiness insight

2.1 Objective

To establish the first authoritative record of cryptographic usage and exposure across public-sector cloud estates, including managed third-party and SaaS integrations. Outputs can be directly consumed by CISOs, architecture boards and external assurance teams.

This service is delivered strictly in accordance with G-Cloud Lot 3 (Cloud Support) requirements, where the Buyer retains full operational responsibility and decision-making authority. Zanloop provides advisory, guidance and support services only, and does not operate, manage or deliver live services on behalf of the Buyer.

This service is designed for public sector security leaders, enterprise architects, cyber assurance and risk owners.

2.2 Detailed Activities

Estate engagement and scoping

• Workshops with application, cloud platform, DevOps, and cyber stakeholders
• Alignment to classification, long-retention data and regulatory context

Technical discovery (non-intrusive)

• Encryption at rest configuration
– Azure Blob, AWS S3, GCP Storage
– Managed SQL, NoSQL, serverless data services
– Analytics platforms and event streaming
• Data in transit
– TLS/MTLS configuration
– Service mesh identity patterns
– Internal and external API endpoints
• Identity and secrets
– Token signing and verification mechanisms
– Key vault usage, HSM or KMS integration
– Federation trust boundaries and exposure
• Certificates and key material

– Chain trust, expiry, automation integrity
– CSP crypto defaults and responsibility mapping
• Container and serverless environments
– Crypto libraries, dependency tracing

Artefact extraction and assessment

• Algorithm and key-size validation
• Cipher-suite negotiation and downgrade risks
• Deprecated hashing or key-exchange
• PQ-risk indicators for high-retention or exposed systems

2.3 Deliverables

• **Encryption Library** — structured artefact (Excel/CSV) capturing full cryptographic estate and ownership
• **Cryptographic Control Mapping Notes** — governance and responsibility model
• **PQ Exposure Snapshot** — quantum vulnerability indicators
• **Executive Summary Findings Report** — for governance and audit

Deliverables will be provided in a reusable format suitable for direct actioning (typically a Word report accompanied by structured data artefacts such as spreadsheets or architecture diagrams).

2.4 Outcomes

• Proven visibility for cryptographic accountability
• Immediate clarity on highest PQ risk exposures
• Foundation for deeper assessment and secure transition planning
• Reusable assurance artefact

2.5 Assumptions and Boundaries

• Buyer provides access to artefacts and change-history where needed
• No exploitation, penetration testing or operational takeover
• Advisory Cloud Support only

3. Public Sector Alignment and Value

These services directly support:

• Government Cyber Security Strategy delivery
• NCSC guidance on crypto discovery and secure transition
• Zero Trust architecture reinforcement across cloud services
• Public-sector long-retention data protection requirements
• Ministry of Justice, Home Office and NHS operational resilience objectives
• Defence and national security controls requiring cryptographic assurance
• HM Treasury spend and risk assurance
• Local authority cloud transformation and data protection alignment

They provide measurable value through:

• Reduction of systemic cryptographic fragility
• Oversight, transparency and accountability across cloud supply chains
• Priority-driven transformation aligned to mission impact
• Improved assurance evidence for audit and regulatory scrutiny
• Prevention of future operational disruption due to quantum risk

---

4. Who Benefits

• Chief Information Security Officers (CISO)
• Senior Information Risk Owners (SIRO)
• Chief Architects and Design Authority chairs
• Cloud platform owners and operations teams
• Service owners accountable for critical citizen services
• Data owners responsible for long-retention confidentiality
• Governance, audit and compliance authorities

---

5. Delivery, Support and Engagement

• Work delivered during **UK business hours** (Mon–Fri)
• Collaboration through secure Buyer-approved channels
• Workshops scheduled with identified stakeholders
• All deliverables stored in Buyer-owned repositories
• No sensitive or official data removed from Buyer control
• Documentation integrates with existing governance formats

Cyber Essentials (or equivalent) can be obtained in line with framework requirements and buyer call-off conditions. Staff clearance will be obtained as required (BPSS or SC).

---

6. Onboarding Process

• Kickoff briefing with Buyer’s programme and risk owners
• Initial request for existing artefacts and cloud tenant information
• Agreement of scope boundaries aligned to governance controls
• Creation of a Delivery Plan with activities, owners and timelines
• Early identification of stakeholders and decision points
• Clear data management responsibilities established from the outset

Onboarding is **lightweight** — designed to accelerate value generation.

---

7. Offboarding and Knowledge Transfer

• Review of deliverables for completeness and accuracy
• Knowledge transfer sessions to operational and governance teams
• Optional handover to other suppliers supporting migration phases
• Removal of access permissions and destruction of temporary working data
• Buyer retains **all** intellectual property and artefacts created under call-off

Capability uplift ensures **no ongoing dependency** on Zanloop.

---

8. Accessibility

All deliverables can be produced in accessible formats consistent with UK public sector accessibility guidance, including:

• Screen-reader compatible document formats
• Clear structure, headings and reading order
• Alt-text descriptions where diagrams or visualisations are used
• High-contrast and dyslexia-friendly formatting options

Workshops can be delivered with **interpreters or captioning** on request.

---

9. Performance and Availability

This is a consultancy and advisory service, not a hosted solution — so performance and availability relate to:

• Consultancy scheduling
• Timely delivery of agreed milestones
• Responsiveness to governance requests
• Quality assurance review of all artefacts and outputs

No 24×7 SLA or operational service scope is included under Lot 3.

---

10. Data Protection and Security

• No Buyer data is stored outside Buyer-approved locations
• No sensitive operational data removed from Buyer control
• All information handled under appropriate confidentiality agreements
• Access limited to authorised personnel for delivery duration only
• All staff adhere to UK data protection legislation and contractual controls
• Data classification handled under Buyer policy and oversight

Where required, we will align to:

• Official-sensitive data handling restrictions
• Secure collaboration environments
• Specific cloud tenancy access controls

---

11. Cloud Targeting and Technology Compatibility

• AWS, Azure, GCP and government-approved hosting (hybrid supported)
• Workload types include: serverless, containerised, platform-managed and SaaS-integrated
• Cryptographic architecture aligned to CSP best practice patterns
• PQC-hybrid integration assessed against available technology readiness

No CSP privileged access is required under this service.

---

12. Reporting and Governance

• Clear status communication for each engagement
• Artefacts designed to support governance bodies including Architecture Review Boards, Design Authorities, SIRO oversight and Audit Committees
• Evidence aligned to ICS assurance requirements and NCSC guidance
• Traceable findings and recommendations with explicit ownership
• Enterprise architecture integration where required

---

13. Pricing and Commercial Terms

Pricing is handled separately under the required G-Cloud rate card.
No pricing content is included in this catalogue description.

---

14. Security Clearance and Assurance

• Staff clearance (BPSS or SC) obtained as required
• Clear separation between advisory services and operational access
• Zanloop **does not** provide SOC or incident response
• Zanloop **does not** take possession of cryptographic keys
• Zanloop **does not** operate or monitor live services

---

15. Compliance and Support Commitments

Zanloop provides support during UK business hours (Monday–Friday) as standard under this service. Where a Call-Off Contract requires extended or 24×7 support, or specific security clearance levels, Zanloop will provide such support subject to agreement and appropriate lead times.

Zanloop commits to ensuring that all personnel involved in delivery meet the security and vetting requirements specified by the Buyer on a per-engagement basis (for example, BPSS or SC). Where additional resourcing is required, suitable cleared personnel will be provided via trusted delivery partners under subcontractor status notified at Call-Off award.

Cyber Essentials
In line with G-Cloud framework requirements, Zanloop will obtain Cyber Essentials certification within the required timeframe where this is applicable to the services being delivered. Where a Buyer specifies additional assurance requirements, including Cyber Essentials Plus, Zanloop will work with the Buyer to agree appropriate assurance arrangements prior to the commencement of the Call-Off.

---

16. Lot 3 Cloud Support Compliance Declaration

These services **do**:

• Support cloud enablement, secure design, cryptographic assurance and PQ readiness
• Deliver discovery, advisory, architectural design, migration enablement and governance uplift
• Transfer knowledge and capability to the Buyer
• Respect that the Buyer retains full operational control
• Apply exclusively within a cloud-support context

These services **do not**:

• Host or operate cloud services
• Provide IaaS, PaaS or SaaS products
• Deliver penetration testing, CHECK, incident response or SOC services
• Provide key-management operations
• Commit to 24×7 service operation
• Take responsibility for change approval or live deployment decisions

They are fully aligned to G-Cloud 15 **Lot 3: Cloud Support** rules.