

Digital Transformation & Support for Hosted Public Safety & Policing Systems

Service Definition: G-Cloud 15 – Lot 3

1. Introduction

Public safety and policing organisations increasingly rely on hosted and cloud-based digital platforms to deliver operational, investigative and enabling services. These platforms include records management systems, command and control, intelligence and investigation systems, digital evidence services, analytics and reporting tools, and associated integrations delivered through SaaS and hosted models.

Operating and changing these platforms requires a strong focus on assurance, security, data integrity and operational readiness, particularly within policing environments subject to accreditation, governance and regulatory oversight. Poorly controlled digital change can create material risk to service continuity, public confidence and statutory compliance.

This service provides cloud-enabled digital transformation and assurance support to help public safety organisations safely review, implement, transition, optimise and govern hosted digital platforms, including the appropriate use of DevOps practices to enable reliable and repeatable delivery. Delivery focuses on controlled change, risk reduction and readiness for live operation, supported by modern delivery practices and tooling where appropriate.

Services are delivered as defined, outcome-based pieces of work aligned to statements of work and buyer requirements under G-Cloud 15 Lot 3.

2. Service Overview

The service supports police forces, national policing bodies and other public safety organisations operating hosted or cloud-based digital platforms, as well as those transitioning from on-premise or legacy environments to SaaS or hosted operating models.

Typical platforms include hosted records management systems (RMS) such as Niche RMS, Athena, Connect and Storm, alongside command-and-control systems, intelligence and investigation platforms, digital evidence management systems, analytics and reporting solutions, and associated integration services.

The service focuses on the delivery, improvement and governance of public safety digital services operating on hosted platforms. It supports organisations to maximise the value of

investment in core systems while maintaining operational assurance, security, data integrity and regulatory compliance.

The service is delivered independently of software suppliers. While maintaining strong, constructive working relationships with platform vendors, delivery is focused on supporting the best outcomes for the organisation.

All services are delivered as defined, time-bound pieces of work under an agreed Statement of Work. This service does not include ongoing system administration, managed service provision, BAU helpdesk activity, operational delivery or delegated statutory decision-making. The buyer organisation retains full ownership and responsibility for its systems, data and live service operations at all times.

All Futures personnel follow secure onboarding and offboarding processes and operate under role-based access controls. Where required, Futures may process personal or sensitive data strictly on behalf of the buyer organisation, with access minimised, time-limited and granted only where explicitly authorised. Futures does not host or independently store customer data; all data access and processing is undertaken within the buyer's secure environments, systems and governance arrangements.

Delivery aligns with cloud shared responsibility principles, recognising the respective roles of platform vendors, the buyer organisation and Futures. Futures provides advisory, delivery and enablement support only and does not take responsibility for operating, hosting or administering customer cloud platforms.

3. Security, Assurance & Operating Context

Delivery within public safety environments requires a clear understanding of security, accreditation and assurance requirements. Services are delivered with due regard to:

- Appropriate security clearances held by delivery staff.
- Secure handling of sensitive operational and personal data.
- Alignment to policing security standards, accreditation and governance frameworks.
- Organisational assurance, audit and compliance requirements.

Assurance considerations are embedded throughout discovery, design and delivery activity. This ensures digital change is safe, controlled and operationally ready, rather than treated as a purely technical exercise.

4. Health Checks & Discovery

Purpose:

To establish a clear, evidence-based understanding of how existing public safety platforms support operational delivery and to identify risks and priorities for improvement.

Activities:

- Review of current system configuration, usage and constraints.
- Assessment of data quality, information flows and reporting.
- Review of integrations between public safety systems and partner organisations.
- Discovery sessions with operational, technical and assurance stakeholders.
- Identification of risks, dependencies and improvement opportunities.

Outcomes:

- Shared understanding of current strengths and limitations.
- Clear definition of improvement and transition priorities.
- Evidence-based inputs to inform options and delivery planning.

5. Options Analysis, Business Case & Procurement Support

Purpose:

To support informed decision-making and secure approval for change through proportionate analysis, business case development and procurement support.

Activities:

- Options appraisal and impact assessment.
- Service, data and integration design options.
- Benefits identification and value assessment.
- Risk, dependency and affordability analysis.
- Support to framework call-off and procurement approaches.
- Mobilisation and readiness planning.

Outcomes:

- Clear, evidence-based options.
- Decision-ready business case material.
- Agreed delivery and mobilisation approach.

6. Implementation & Delivery Support

Purpose:

To support the effective implementation, improvement or optimisation of public safety digital platforms through clearly defined delivery workstreams.

Typical Delivery Workstreams:

Support can be provided for all, or a selected subset, depending on in-house capacity and maturity:

- **Programme and Project Management** – planning, governance, dependency management and reporting.
- **Operational Change Management** – stakeholder engagement, communications and adoption support.
- **Business Analysis** – requirements definition and translation into system configuration.
- **Configuration and Platform Assurance** – governance and assurance of system configuration and hosting arrangements.
- **Data Migration and Data Quality** – migration strategy, preparation, testing and cutover support.
- **Testing & Readiness Assurance** – test coordination, validation and operational readiness sign-off
- **Reporting & Analytics** – operational, performance and management information
- **DevOps and Delivery Enablement** – advisory and enablement support for the use of DevOps practices, automation and modern tooling to improve consistency, assurance and repeatability of delivery activity, implemented within policing security, accreditation and governance constraints
- **Training & Enablement** – training delivery and user support.

Delivery is provided through multi-disciplinary delivery teams, drawing on specialist contractors engaged to deliver defined outcomes within agreed statements of work.

Outcomes:

- Controlled delivery aligned to organisational capacity.
- Reduced delivery, data and assurance risk.
- Platforms configured and adopted to support operational policing needs.

All configuration, data and workflow activity undertaken by Futures is time-bound, project-specific and delivered in accordance with an agreed Statement of Work and the buyer organisation's governance arrangements. Futures does not provide ongoing system administration, managed service provision or operational ownership of customer systems.

7. Digital Enablement & System-Adjacent Innovation

Purpose:

To provide digital enablement support that complements and extends core platform-related activity, delivered either alongside wider system delivery or as a standalone, defined piece of support.

Scope of Support:

Where directly linked to public safety platforms and services, support may include:

- Digital road-mapping aligned to operational priorities.
- Data and insight enablement to support decision-making and assurance.
- Automation and productivity tooling within secure environments.
- Use of existing cloud platform capabilities to improve efficiency and consistency.

All activity is delivered in line with security, assurance and governance requirements.

Any use of AI or automation is implemented only within buyer governance, proportionality and oversight, and does not replace statutory decision-making or operational casework responsibilities.

8. Transition to BAU & Operational Readiness

Purpose:

To ensure public safety digital services are stable, supported and ready for sustainable business-as-usual operation.

Activities:

- Operational readiness and go-live support.
- Support model and escalation design.
- Handover to internal teams and suppliers.
- Performance and service monitoring setup.

Outcomes:

- Stable BAU operation.
- Clear ownership and governance.
- Reduced reliance on external support.

Support focuses on readiness for the defined transition period. Responsibility for BAU operations and live service management remains with the buyer and its system suppliers. This service does not provide ongoing operational support.

9. Post Go-Live Support & Optimisation

Purpose:

To support continuous improvement once services are live.

Activities:

- Configuration and workflow optimisation.
- Performance and reporting refinement.
- Assurance and improvement support.

Outcomes:

- Improved system performance and usability.
- Better alignment with operational needs.

Post go-live support is limited to short, defined pieces of optimisation or assurance work delivered under an agreed Statement of Work. It does not constitute a retained, ongoing or continuous support service.

10. Knowledge Transfer & Capability Building

Purpose:

To embed digital capability within public safety organisations.

Activities:

- Structured knowledge transfer and documentation.
- Coaching and mentoring.
- Support to internal capability development.

Outcomes:

- Sustainable in-house capability.
- Reduced long-term dependency on external support.

11. Delivery Approach & Governance

Services are delivered through defined statements of work aligned to buyer requirements. Delivery is supported by clear governance, reporting and assurance arrangements proportionate to the size and complexity of each engagement.

Support can be provided across individual workstreams or end-to-end, depending on organisational need and capacity.

12. Social Value

Social value is delivered through structured knowledge transfer, skills development and clear documentation that support staff to operate and improve public safety systems.

Delivery promotes resilient digital operating models, improved data quality and insight that support safer communities, and reduced reliance on external support over time. Where aligned to organisational objectives, improved digital efficiency can also support more sustainable ways of working.

13. Ordering & Engagement

This Services are available via G-Cloud 15 Lot 3 call-off. Engagements are defined through agreed statements of work setting out scope, deliverables, timescales and outcomes.

14. Summary

This service supports public safety and policing organisations to adopt, stabilise, improve and govern hosted digital platforms. It focuses on cloud-enabled transformation delivered with strong assurance, security and operational readiness to support effective and sustainable policing outcomes.