HCLTech | Supercharging Progress™

G-Cloud 15 – RM1557.15

Lot 2b - Software as a Service

PROTECT - Records Management System

Service Description

G-Cloud 15 - Lot 2b Software as a Service - Records Management (Police) - Service Description

Foreword

This proposal has been prepared by HCLTech, for the sole use of Crown Commercial Service (CCS). The contents of this document shall remain the confidential property of HCLTech and should not be communicated to any other party without the prior written approval of HCLTech.

The furnishing of this document shall be subject to contract and shall not be construed as an offer or as constituting a binding agreement on the part of HCLTech to enter into any relationship.

HCLTech warrants that, to the best of their knowledge, those who prepared this document have taken all reasonable care in preparing it, have made all reasonable enquiries to establish the veracity of the statements contained in it and believe its contents to be true. (HCLTech cannot however warrant the truth of matters outside of its control and accordingly does not warrant the truth of all statements set out in this document to the extent that such statements derive from facts and matters supplied by other persons to HCLTech. The statements in this document are qualified accordingly.)

Validity

This proposal and all information contained within are valid for a period of 180 days from January 30, 2026.

HCLTech Contact

Name	Paul Montgomery
Address	6th Floor 70 Gracechurch Street London EC3V 0XL
Email	eas-hclsalessup@hcltech.com or Paul.Montgomery@hcltech.com
Phone	+44 (0) 7747 828480 or +44 (0) 20 7105 8600

G-Cloud 15 - Lot 2b Software as a Service - Records Management (Police) - Service Description

Table of Contents

About HCLTech 1

Service Description 1

Solution Overview ..... Error! Bookmark not defined.

Features 4

Benefits 6

Technical Specifications 6

Implementation 7

Support Arrangements 9

Business Continuity/ Disaster Recovery 10

Data Backup/ Restore ..... Error! Bookmark not defined.

Security 10

Exclusions 11

Account Management 11

G-Cloud 15 - Lot 2b Software as a Service - Records Management (Police) - Service Description

About HCLTech

HCLTech is a next-generation global technology company that helps enterprises reimagine their businesses for the digital age. Our technology products, services and engineering are built on four decades of innovation, with a world-renowned management philosophy, a strong culture of invention and risk-taking, along with a relentless focus on customer relationships.

With a worldwide network of Research and Development (R&D), innovation labs and delivery centres and over 225,000+ 'Ideapreneurs' working in more than 60 countries, HCLTech serves leading enterprises across key industries. HCLTech generated consolidated revenues of USD 13.8 billion for 12 Months ended 31st March 2025 with 4.5% Increase YoY. For latest figures, please refer to the link below:

About our Company: HCLTech – Supercharging Progress
HCLTech' s Annual Report 2024-25 | HCLTech

We offer an integrated portfolio of products, solutions, services, and Intellectual Property (IP) through our Mode 1-2-3 strategy built around Digital, Internet of Things (IoT), Cloud, Automation, Cybersecurity, Analytics, Infrastructure Management and Engineering Services, amongst others, to help enterprises reimagine their businesses for the digital age.

Service Description

HCLTech's PROTECT is a modern, scalable, and highly intuitive Records Management System (RMS) designed in close partnership with UK Policing that offers a future-ready, user-focused alternative to legacy RMS platforms. Case, Custody, Investigation, Stop & search and Intelligence, PROTECT enables seamless, efficient Policing workflows supported by unmatched data quality, automation, and mobility capabilities.

PROTECT is a next-generation platform designed to unify and streamline core policing processes. Built for UK police forces, it combines advanced functionality with cutting-edge AI to deliver efficiency, accuracy, and security. It has been designed to follow national standards, policies, and guidelines with well-integrated with the force's local and national systems. PROTECT has been designed and implemented considering multi-tenancy which can be easily enabled for any police force and requires minimal configuration changes.

The solution is flexible which allows Forces to implement custom variations while preserving a consistent data schema. PROTECT can be quickly reconfigured to meet changing requirements at little to no cost. Despite our size and global reach, every aspect of PROTECT's design and functionality was built from the ground up for this market alone, to maximise frontline productivity and mission impact. Nothing has been retrofitted or repurposed from other jurisdictions; everything was co-designed with front line staff from UK Forces.

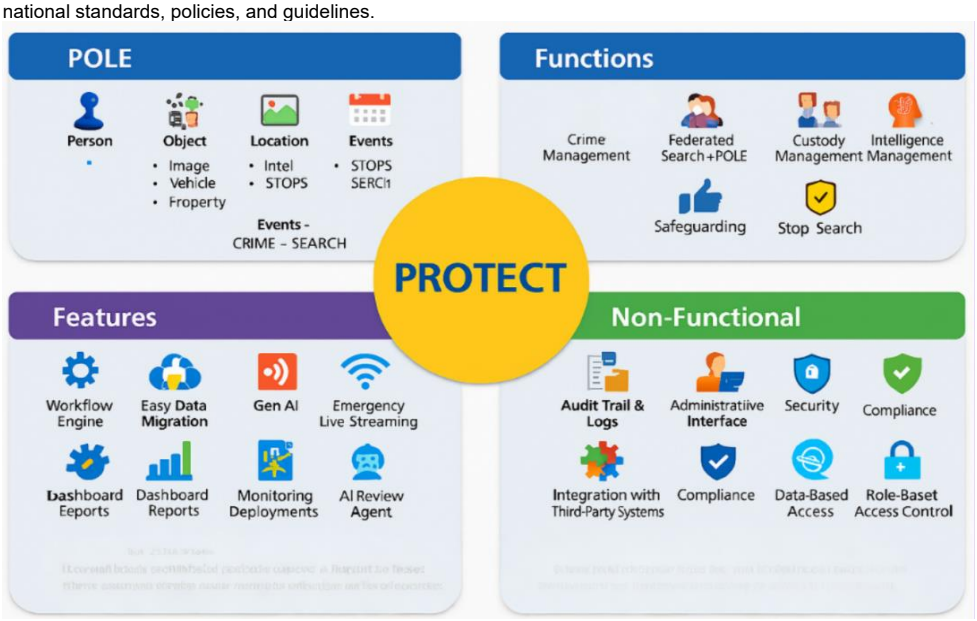
AI-Powered Enhancements
PROTECT leverages advanced Artificial Intelligence to transform policing operations. Integrated Facial Recognition technology enables rapid and accurate identification of individuals from images, significantly improving investigative efficiency. Our Generative AI capabilities allow officers to perform intuitive, conversational searches across records—whether looking for a person, object, location, or event—delivering faster data retrieval and actionable insights.
Beyond these core features, PROTECT offers powerful AI-driven capabilities:

- **Crime Classification Recommendation** for accurate categorization of cases.
- **PDF Redaction** to securely remove sensitive information.
- **Facial Recognition:** to identify individuals
- **Document Summariser & Q&A** for quick understanding of lengthy files.
- **Document Scanner** with OCR for seamless digitisation.
- **Vehicle Plate Detection** for real-time tracking and intelligence gathering.
- **Case Solve Prediction** to forecast the likelihood of cases getting solved within a specified timeframe allocation
- **Review Agent:** CPIA-compliant identification of incorrect or missing process information and advises prompt submission of all relevant details to maintain accurate investigation and disclosure standards

G-Cloud 15 - Lot 2b Software as a Service - Records Management (Police) - Service Description

Solution Overview

HCLTech's PROTECT solution manages the records of various policing business processes right from initial data capture to completion. It is designed on a POLE concept managing the information of the core policing entities: person, organisations, locations, vehicles, objects, incidents, and events. This has been designed to adhere to national standards, policies, and guidelines.



Here is a list of the current functionalities present within the solution and is growing as per the product roadmap and on demand basis:

Person, Object, Location and Event(POLE) search: POLE Search is an advanced Gen AI-powered capability that enables officers to query interconnected intelligence data across multiple platforms. By consolidating information about Persons, Objects, Locations, and Events, it provides a holistic view of incidents and associated entities. This feature supports rapid decision-making, operational efficiency, and cross-linking of suspects, witnesses, victims, and events such as arrests or intel reports. Officers can use natural language queries for quick and intuitive searches, ensuring timely access to critical information.

Natural Language Search (Gen AI) **:** Users can type queries in plain English (for example, "Show all urgent cases for my team this week"), and the system interprets and executes them

Facial Recognition : Facial Recognition in PROTECT uses advanced biometric algorithms to identify individuals by analyzing facial features from images or videos. It detects faces, extracts unique characteristics, and compares them against a database of known faces, including custody imagery. Integrated with national systems, it supports federated searches and enables officers to upload photos or select images from case files for quick identification. This capability accelerates investigations, especially when traditional identifiers like names or IDs are unavailable.

Federated Searches: Federated Search in PROTECT allows officers to perform comprehensive queries across multiple systems, including PNC, PND, and intelligence databases, without logging into each individually. Results

are presented in a unified view, ensuring data consistency and accuracy. This feature eliminates silos, streamlines workflows, and enhances operational efficiency. By integrating national-level intelligence, it supports critical decision-making for investigations, incident response, and strategic planning

Network Diagrams**:** The Network Diagram in PROTECT provides an interactive visual representation of relationships between key intelligence entities such as persons, locations, objects, and events. Using nodes and edges, it illustrates connections like kinship, proximity, and operational roles, supported by visual cues for clarity. This tool enables rapid triage during incidents, helps analysts uncover indirect links, and supports operational briefings with concise summaries. It transforms complex case data into an intuitive, POLE-aligned view for faster, more accurate decisions.

Crime and Investigation Management – PROTECT's Investigation Management module empowers officers with AI-driven crime classification, ensuring compliance and reducing errors. It supports secure communication with victims and witnesses, manages non-crime investigations, and provides analytical tools for uncovering patterns. Features like task management, multi-agency collaboration, and DEMS integration streamline workflows and enhance efficiency. This module significantly reduces crime recording time, enabling officers to focus on critical tasks.

Intelligence Management – Intelligence Management module ensures timely access to critical information for frontline and specialist officers. It delivers full lifecycle management aligned with the National Intelligence Model (NIM) and enables intelligence reports to be submitted directly from the field using mobile devices. The module supports 3x5x2 grading and source evaluation, ensuring data accuracy and reliability. Facial recognition links surveillance images to POLE data, helping identify suspects and uncover networks. Organized into intuitive sections—My Intel, Create Intelligence, and Search Intelligence offers advanced filtering and retrieval capabilities for comprehensive situational awareness.

Case Management – The Case Management module in PROTECT supports the complete lifecycle of criminal cases, from initial investigation to court outcomes. Compliant with DCF and TWIF standards, it enables seamless electronic case preparation, document generation, and management of defendants, witnesses, and exhibits. Automated updates keep victims and witnesses informed, while adaptable workflows and court-ready form generation save time and ensure compliance. This module enhances collaboration across CJS partners for efficient case progression.

It has the capability of supporting advanced resource planning as well in addition to automatically sending updates to victims and witnesses. It also Supports pre-charge, postal requisition, and Police-led prosecutions with adaptable workflows to match Force processes. The case management system is capable of readily generating court-ready forms, including all MG documents, using Force-specific templates, saving front-line staff time.

Custody Management - PROTECT's Custody Management module ensures secure and compliant detainee handling in line with PACE regulations. It reduces cognitive burden on staff through intuitive interfaces and tailored automations, supporting effective risk management and better welfare outcomes. Designed for high-pressure environments, this module assists supervisors in making informed decisions while minimizing operational risks in custody suites.

Safeguarding – PROTECT ensures to provide features and functionality to assist forces in protecting children and vulnerable adults from abuse and maltreatment. Missing Person, child protection, vulnerable adults and domestic abuse are some of the offerings which cover major safeguarding areas around vulnerable citizens.

Stops & Search - This offering has the functionality to create and capture vehicle, and person or person only stops. Officers have the capability to capture details pertaining to the encounter: stop location, address, personal and vehicle details, powers used and intelligence obtained. Officers have the capability to generate printed records in real time. The application also allows officers to create clone tickets/ records with similar details to avoid rework and save time.

The other modules in PROTECT include Problem Solving, Sudden Death Reporting, etc. HCLTech PROTECT is designed to be able to accommodate the future business needs of the force, ensuring that new business processes can be added, and existing processes can be enhanced with less effort.

Features

PROTECT is designed to meet the Records Management System (RMS) requirements of the policing sector and aims to meet the latest market trends and requirements. PROTECT has been designed to support cloud, in-house and hybrid hosting platforms. All technologies, framework, patterns, and services used to develop PROTECT are compatible with cloud.

Key features of respective modules are listed below:

Key Investigation Management capabilities include:

- **AI Crime Classification**: Ensures compliance with Home Office Counting Rules (HOCR) and reduce human error while improving consistency in crime data reporting.
- **Victim and Witness Communication**: Built-in portal enables secure two-way contact via email, SMS, or letter using pre-approved templates that promote clarity, consistency, and compliance.
- **Support for Non-Crime Investigations**: Manages cases such as anti-social behaviour and missing persons for a comprehensive public safety approach.
- **Data Analysis and Visualisation**: Provides network charts and analytical tools to help investigators uncover patterns and relationships in crime and ASB data.
- **Task Management**: Allows investigators to assign and monitor tasks, supporting timely and efficient case progression.
- **Multi-Agency Collaboration**: Integrates with external systems to enable secure, low-friction data exchange and improved joint outcomes.
- **Remote Witness Statements**: Supports remote statement capture and digital signature via a secure portal, enhancing efficiency and compliance.
- **Digital Evidence Management System (DEMS) Integration**: Seamlessly connects with any DEMS for access to linked digital evidence.

Key Case Management features include:

- **Customisable Workflows**: Supporting pre-charge, postal requisition, and Police-led prosecutions with adaptable workflows to match Force processes.
- **Automated Documentation**: Readily generates court-ready forms, including all MG documents, using Force-specific templates, saving front-line staff time.
- **Integrated Redaction**: Simplifies evidence preparation with our built-in smart redaction tooling that reduces the burden of disclosure and court submission.
- **Exhibit Management**: Enables detailed logging of exhibits to support investigation integrity and prosecution readiness.
- **Integrated Messaging**: Facilitates communication with courts, CPS, victims, and witnesses - including Two-Way Interface (TWIF) integration with HMCTS and CPS.
- **Task Management**: Assigns, tracks, and manages tasks such as responding to CPS memos, disclosure handling, and witness coordination.
- **Case solve prediction**: Utilises advanced AI models to analyse historical case data and investigative patterns to predict the likelihood of case resolution. This helps prioritise efforts, effectively, and improve overall case management efficiency.

Key Custody Management capabilities include:

- **Custody Whiteboard:** Provides a live visual overview of all detainees, enabling real-time monitoring of status, movements, and welfare needs.
- **Seamless Intake Process:** Smooth transition from arrest to custody ensures accurate, compliant entry into the system.
- **Risk and Welfare Logging:** Captures detainee risk factors, medical needs, and personal property to support safety and accountability.
- **Movement and Event Tracking:** Tracks internal movements, facility transfers, interviews, and medical visits with fast, intuitive logging to maintain a complete custody record.
- **Automated Alerts:** Reminds Officers of legal review deadlines, detention limits, and required authorisations, supporting compliance with custody regulations.

Key Intelligence capabilities include:

- **Mobile Intelligence Capture**: Enables secure, on-the-go submission of multi-media intelligence, ensuring timely and accurate sharing from the field.
- **Automated Routing**: Submissions are automatically directed to the appropriate teams based on pre-defined workflows and risk profiles.
- **Intuitive Grading and Evaluation**: Simplified interfaces support consistent grading, source evaluation, and risk assessment.
- **Advanced Search Tools**: Enables powerful, user-friendly searches using filters, keywords, metadata, and thematic tags.
- **Visual Analysis**: Link analysis and association mapping tools provide visual insights improving situational awareness.
- **Tasking and Alerting**: Intelligence teams can assign tasks and set up automated alerts for pre-defined risks or priority entities, ensuring rapid response to emerging threats, improves operational efficiency, and reduces the risk of missing critical intelligence by proactively notifying relevant personnel and enabling targeted follow-up actions.
- **Multi-Agency Collaboration**: Secure, auditable integrations facilitate compliant intelligence sharing with partner agencies.
- **Vehicle Plate Detection :** Enables real-time identification and tracking of vehicles, supporting intelligence gathering, surveillance, and investigative workflows

Some additional features:

- **AI-Supported Data Quality Controls:** Innovative machine learning models trained against Home Office Crime Recording Rules assist users by recommending appropriate crime classifications. AI-assisted entity matching will identify potential duplicate POLE records and supports controlled, auditable merging actions, with all links reassigned to a master record. Scheduled background scans work to identify anomalies such as orphaned or incomplete records for administrative review.
- **Smart Controls and Automated Validations:** Dynamic picklists, predictive text, and mapped dropdowns guide users through data entry. These controls suggest or auto-fill values based on existing records, reducing errors and improving consistency.
- **Audit Logging and Error Handling:** Comprehensive audit logs record all data changes, access events, and user actions, supporting accountability, non-repudiation, and post-incident analysis. A structured error-handling framework provides clear, actionable messages to users, helping them correct issues quickly and maintain data quality and integrity.

- **Consistent Cross-Device Experience:** A consistent user experience across desktop and mobile devices ensures Officers can access and update records efficiently, regardless of location.
- **Automated Notifications and Visual Guidance:** Automated alerts, workflow prompts, progress indicators, and visual cues ensures users stay on track, reduce missed steps and significantly improves productivity.
- **Automatic Victims' Code (VCOP) Update** – PROTECT provides auto-generated notifications for victims of crime at the point of submission via email and/or text. This provides support information for victims and enables the Force to better comply with its duties under the Code.
- **Quick Links** – Quick links for the frequently used entities within the application have significantly saved time in the crime recording process.
- **Data Reuse and Pre-Population:** The system drives data reuse by pre-populating fields from existing records (for example, an incident, a custody record), cloning events, and auto-populating related entities (defendants, victims, witnesses). This minimises redundant data entry and enhances accuracy and efficiency.
- All business processes and systems are integrated for seamless data flow. Automation is in place to pre-populate most fields in the background.
- **Supports Data Migration** – The application supports easy data migration from the force's current RMS into Protect.

Benefits

- Huge time savings, (40-45% time reduction in crime recording).
- Improved service to victims – automated updates to victims.
- Vastly improved user experience – the solution needs no training and pop-up windows help to enable officers to carry out their tasks.
- Improve data quality – a welcome by-product of the system's introduction.
- Contextual prompts and validations that confirm the next logical step in a workflow, helping to prevent errors at the point of entry and improving data quality
- Tooltips and inline explanations that clarify the purpose of fields, actions, and decision points without requiring the user to leave the screen or consult a manual
- Auto-save and transactional integrity that protect the user's work during mobile use or moments of network disruption
- Simplified views and focus modes that reduce distractions and highlight the immediate task, particularly important for Officers working in fast-moving situations
- Smart suggestions such as predictive text and AI-assisted writing that support report drafting, will reduce spelling and grammar errors, and help user's complete forms more quickly.
- Adaptive support features that adjust based on role, device, and task type, removing unnecessary options and reducing the likelihood of confusion

Technical Specifications

PROTECT adheres to a Service Oriented Architecture (SOA) style which enables loose coupling among the components. The solution is highly scalable, configurable and supports a multi-tenant environment. The SOA architecture helps to get data from the Force's local and national policing systems via integration services. The architecture also follows appropriate data standards, uses extensible open standard technologies such as SOAP based services and provides shared, reusable and extendable services.

PROTECT comes with a Single Sign-On (SSO) framework. This is an authentication process which allows police officers to access multiple applications with a single set of login credentials.

With single sign on, officers can access all areas of functionality that require integration with other backend systems and they can work on multiple different systems, each with separate login credentials, seamlessly and without repeatedly inputting different systems passwords. This framework eliminates the need to re-enter the third-party systems credential each time. The officer just enters their police system credentials once into the PROTECT application or those could be authenticated with force AD.

PROTECT's presentation components interact internally with the business layer for business process execution. They do this by calling a RESTful (Representational State Transfer) service API (an interface that two computer systems use to exchange information securely over the internet), which in turn calls a business interface. The business interface implementations encapsulate PROTECT's business components by using logically grouped business facades. Also, as PROTECT follows microservice and multi-tenant architecture, business logic implementation for each tenant force is separated by further extending the common business interface or via an abstraction pattern.

The application layer comprises business interfaces (for dependency injection) and corresponding implementation components, business classes with rule validations, workflow classes, reporting logic and Web API proxy for repository services invoking.

Interoperability is a key characteristic of PROTECT, supporting and enabling its seamless integration with different policing systems or third-party applications

Implementation

HCLTech will deliver the implementation of the multi-force PROTECT RMS through a controlled, collaborative, and transparent delivery approach. The model will be grounded in close partnership with the forces, using co-located and cross-functional teams to ensure decisions are made with operational insight and that delivery remains aligned to frontline policing realities throughout the programme lifecycle.

Approach to Force Implementation

PROTECT is engineered to support single/multi-force deployment without complexity or compromise. Its Situational Layer Cake architecture separates shared capabilities from local variation, with consortium and cluster layers providing common services such as security, audit, and UI standards, while force-specific layers allow local workflows, templates, and compliance rules to be applied independently. This ensures forces can operate differently where needed without fragmenting the platform or creating parallel builds.

This is reinforced by PROTECT's Service-Oriented Architecture (SOA), where core functions such as Case Management, Custody, Crime Investigation and Intelligence are delivered as independent modules. Modules can be deployed, updated, and fixed in isolation, enabling phased onboarding, controlled change, and rapid issue resolution without disrupting live forces.

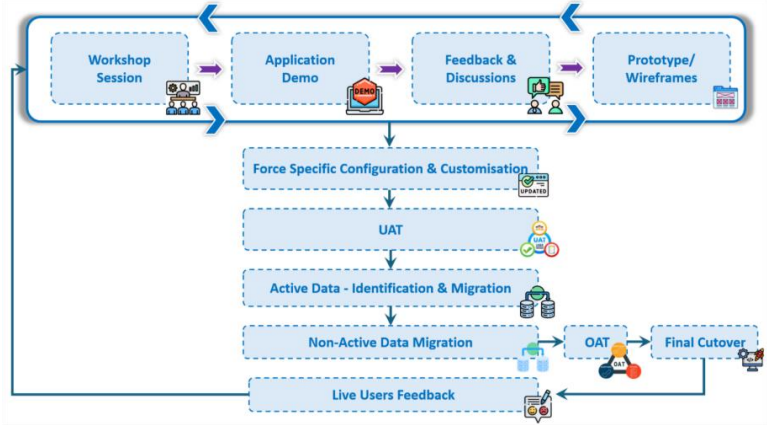
Multi-tenancy is enforced consistently across infrastructure, data, business logic, and presentation. Logical isolation, tenant-level data controls, runtime configuration, and tenant-aware audit and monitoring ensure strict separation, security, and evidential integrity, while still benefiting from shared infrastructure and economies of scale.

How This Architecture Supports Implementation

- **Smooth Phased Rollout:** Multi-tenancy and isolation let each force onboard independently, reducing dependencies.
- **Safe Local Variation:** Configurable layers enable force-specific branding and workflows without custom builds.
- **Reduced Migration Risk**: IAM controls, segmentation, and row-level security prevent cross-tenant exposure.
- **Improved Assurance:** Tenant-aware logging and audit deliver full traceability and faster issue resolution.
- **Faster Testing:** Modular components allow parallel validation and quicker onboarding.

.

The high-level chronological representation of the project level execution activities is provided below.



Force specific Cutover approach

Implementation Plan
A detailed implementation plan demonstrating key deployment stages, activities and resourcing requirements for the complete project can be provided to the customer on request. All the key dependencies will also be identified against the activities in the project plan.

Key dates in a detailed project plan will incorporate:

- Key project phases - for example Scoping, Construction, UAT (User Acceptance Test) and Deployment
- Project deliverables, milestones and quality standards
- Detailed work packages, tasks and dependencies
- Responsibility and accountability for deliverables
- Resource assignment and ownership
- Partner obligations and dependencies.

Risk Planning and Mitigation

Managing and minimising risk is a key element of HCLTech's approach to managing large scale programmes, projects and services. We propose a joint (customer and HCLTech) team to manage risk through a formal, structured framework. This will ensure that vulnerabilities, risks, and threats can be identified and managed/ avoided throughout the project lifecycle and service contract. The objective of risk management is to identify and quantify potential risks, then perform mitigating actions (including risk avoidance) before the risk materialises. Risk management processes and tools will be integrated with other activities throughout the project and service contract lifecycle. The analysis matrix is compiled using the following process:

- Identification of risks - brainstorming session by the joint team and input from other sources
- Analysis and ranking using an appropriate scale assessing the probability and impact, with the product of the two indicating an overall score. The higher the overall score, the greater the priority for the identification of sound counter-measures and contingency plans to manage the risk
- Continuous review and re-assessment – the risk matrix is updated as part of the ongoing Risk Management process.

Once identified, a risk will be recorded and managed through its lifecycle, with risk owners assigned for each stage. This provides a sign-off audit trail and manages reporting against due dates, as well as ensuring that relevant discussions, outcomes, and decisions are recorded.

The standard workflow lifecycle for a risk is shown below:

- Risk logged
- Action manager accepted
- Plan defined

- Plan completed
- Closed by owner.

This provides a simple prioritisation of all risks and helps identify the most appropriate level of management required for each item, i.e. items with a low-risk score can be managed within a workstream, whereas items with a high-risk score require input from a Management/ Steering Group level.

The appropriate risk management strategy for a given risk can only be determined following detailed review and discussion.
As part of this, input and options may be sought from a number of relevant sources within (or outside of) the programme/service contract. Based on this information, the risk management process (operating within the broader governance process) can determine the most appropriate strategy from:

- Avoidance
- Mitigation
- Transference
- Acceptance.

Actions or activities are recorded, associated to the risk and tracked to individual completion.

Support Arrangements

Support boundaries / interfaces

HCLTech proposes to provide Level 2 and Level 3 Support as part of this Service. This will be provided via a shared support team using the remote connectivity from HCLTech offices located in Watford, United Kingdom.

The PROTECT solution is underpinned by a comprehensive Information Technology Infrastructure Library (ITIL) based service model. The HCLTech Support Desk will provide the co-ordination of service management activities including:

- Incident management
- Problem management
- Configuration management
- Service level management
- Escalations
- Complaints.

The HCLTech Support Desk operates business hours and on call support for Severity 1 issues.

Officers will raise Protect solution related issues with their internal Helpdesk in a similar way as they would for other issues. The issues will be routed to the HCLTech Support team for resolution.

Service Levels

The baseline service will come with a monthly service availability Service Level Agreement (SLA) of 99.9%.

We provide high levels of resilience and availability and commit to 99% over the contract term.
The Service will be available 365 days a year, 24 hours a day.

Outage and Maintenance

Planned Works are defined as any activities undertaken by HCLTech as part of routine maintenance, and preventative actions to support the continued running of the service.

HCLTech will ensure that we give at least 10 Working Days' notice of any Planned Works affecting client forces.

Customisation

All agreed customisations will be included within the relevant Statement of Works (SoW) and/ or Solution Design Document (SDD) documentation.

Performance attributes

The HCLTech PROTECT Solution has been designed using modern technologies ensure best performance.

Business Continuity/ Disaster Recovery

The availability of core operational systems in Policing is not an abstract technical concern. When an RMS is unavailable or degraded, Officers lose access to critical situational awareness, data and tools they need to keep themselves and the public safe.

PROTECT is designed to meet this need - providing secure, scalable, and highly available services for mission-critical Policing operations. By combining cloud-native architecture, layered resilience, proactive performance management, and proven experience operating large-scale platforms under sustained operational pressure, HCLTech will provide an RMS that maintains availability, protects operational continuity, and evolves safely as operational demands grow over the life of the contract. For Business Continuity reasons, the solution must remain available even in the face of any physical site downtime. We will work with you to ensure that appropriate measures will be in place in the physical architecture to ensure the required business continuity.

Data Backup/ Restore

1. **For in-house installation:** No infrastructure services are being offered as part of this service. We can provide guidance and support, but backup will remain the customer's responsibility and will be managed by the customer's internal IT team.

2. **For Central Hosting**: As part of this service, HCLTech will provide the backup. The backup plan and strategy will be shared during implementation. If any modification is required as per the customer's requirements, then this will be discussed and agreed during the implementation period. The service will be hosted at a secure IL3 (Impact Level 3) compliant data centre. All the backups will be stored in a restricted place where only authorised personnel will have access to those areas.

The service will be hosted at a secure compliant data centre. All the backups will be stored in a restricted area where only authorised personnel have access.

Security

Security is one of the crucial tenets of HCLTech's solution design. Security design of the solution guarantees confidentiality of data while data is in transit or at rest.

PROTECT solution has been designed to deploy in a secure environment and will be made available over HTTPS to the user. End-to-end encryption, role-based access, immutable audit logging, and protective marking enforcement throughout.

HCLTech has implemented a multi-layered security model within PROTECT, incorporating globally recognised standards:

Technology Area	Standards Used
Encryption	PKI model using AES encryption algorithms for secure key management.
Data Security	ISO 27002 standards to control and protect access to sensitive data.
Network Security	PCI-DSS standards for managing network and data security.
Backup and Archive	ISO 27002 code of practice for information security management.

These standards support safe, auditable data handling while maintaining resilience, compliance, and operational continuity.

The essential factors of the solution architecture are:

Access Management

Access to the application will be managed by the Manage Group functionality in the HCLTech Admin Desktop solution. Access for officers will be controlled by the customer's project team and can be revoked directly from the Manage Group function.

Logging & Audit

Commented [SA1]: Need to check

Complete audit trails are maintained with the HCLTech administration module and this information is accessible to administrators via dashboards.

The HCLTech PROTECT solution implements logging at various levels that can be used for audit purposes.

The first level of logging is implemented at the level where every attempt to access the network servers are logged in appropriate log files. The logging at this level provides information on who attempted to access the network and, which device or workstation was used for the access.

Exclusions

The services listed below are out of scope of the contract terms for on premise services

- Infrastructure and associated infrastructure support
- Remote connectivity to enable shared support
- Load balancer configuration
- 3rd party software licences
- External system connectivity

Account Management

Account Manager and Service Delivery Manager will be appointed to discuss and manage issues, changes and enhancements to the service.

The location and extent of their involvement will depend upon the level of the engagement.

HCLTech | Supercharging Progress™

hcltech.com