The Police ICT Company

Appendix 2
Technical Specification

Version 1
September 2020

Confidentiality Notice

This document is intended for the use of the recipient only. Any other person obtaining this document is requested to forward it by registered post to The Police ICT Company Ltd, 33 Queen Street, London, EC4R 1AP

The information contained herein is the property of The Police ICT Company Ltd and is supplied without liability for errors or omissions. No part may be reproduced, disclosed or used except as authorised by contract or other written permission. The copyright and the foregoing restriction on reproduction, disclosure and use extend to all media in which the information may be embodied.

This document contains sensitive information as of the date provided to the original recipient by The Police ICT Company Ltd and is provided in strict confidence.

SERVICES DESCRIPTION

SECTION 1: Introduction

This document is made up of:

1. This Introduction;
2. Services Description;
3. Managing SLAs and KPIs;
4. Service Level Agreements;

Annex 1: Technical Specification;

Annex 2: Anticipated roll-out

The purpose of this document is to set out the intended scope of the Services to be provided by the Supplier to the Police ICT Company Limited (‘the Customer’, the ‘Authority’ or ‘the Company’). This document describes the Services to be provided from the outset of the contract and is intended to be a ‘live’ document that will be continually updated through the Change Control procedure to ensure it reflects the true nature of services to be provided by the Supplier.

The Customer intends to procure and manage an IT Service Management (ITSM) capability from a Supplier, which may be expanded to meet the ITSM needs of the broader policing community. The first major organisation to use this service will be the recently established Forensics Capability Network (FCN). The solution procured by the Customer will offer a broad ITSM capability to deliver the breadth of requirements across the policing community, however the services delivered for each customer, whilst harmonised to the greatest extent possible to deliver best value for all stakeholders, will need to be flexible such that it may be tailored to meet the specific requirements of individual law enforcement stakeholder organisations, initially the FCN. The services described in this document therefore pertain, primarily, to the requirements of the FCN from the point of the Go-Live of their FCN Xchange system (further described below), however it is further intended to evolve to reflect the incremental uptake in user-base, capability and potential other policing organisations.

1.1 Context

The Transforming Forensics (TF) Programme is one of several national police programmes led by the National Police Chiefs Council and funded by the Home Office. A key deliverable of the TF Programme is the Forensic Capability Network (FCN), a new national organisation created to manage and facilitate forensic capability in both the traditional and digital disciplines, which is hosted by Dorset Police for at least 2 years from 1st April 2020.

The FCN acts in direct support of Police Forces across England and Wales plus the National Crime Agency, British Transport Police and other law enforcement bodies. The FCN is the business vehicle supporting business as usual (BAU) capabilities and services, whilst the TF Programme supports transition to BAU, major change and future capability across the forensics landscape.

TF and the FCN work closely with the Police ICT Company as the delivery partner for the ITSM tools, platform and services required to allow collaboration between Forces and suppliers.

In addition to the contracts that have already been awarded for discovery, application and infrastructure development services, the Company will deliver the IT Support & Maintenance requirements for the FCN Xchange solution currently under development.

There is a general intention to create collaborative working relationships between all stakeholders, including with the Supplier and transitioning localised support, to ensure the smooth deployment and delivery of the Services.

1.2 Characteristics of FCN Xchange

The Supplier will provide planning, delivery and maintenance of IT services within the scope of the services described, enabling users to work efficiently and effectively and the business to achieve predictable service delivery. The Forensics Capability Network (FCN) Xchange system consists of a cloud-based environment, assured to hold Official Sensitive data (with the Police handling instructions for data processed as HIGH applied in line with Police Information Assurance Board direction), accessed through an IAMS solution.

The FCN Xchange platform has an event-based architecture that supports multiple microservices, deployed in containers, and managed automatically in terms of scaling on-demand. The FCN Xchange will potentially store large amounts of forensic data, both ready access and in deep freeze. The FCN Xchange will have no integrations enabled in Release 1, but will later integrate with Force systems, via middleware and APIs to push and pull information. A high-level overview of the system is provided at the end of this document.

The Services as listed in Section 2 (Service Descriptions) shall be delivered to the Company as listed in this document. Section 5 sets out the Service Levels Agreements (SLAs) that apply to the services listed in Section 2.

The Supplier should note the following key dates:

Contract Commencement	14th September 2020
Supplier On-boarding and Service Set-up	September 2020 – December 2020
FCN Xchange Go-Live (Release 1)	December 2020 – March 2021
Initial Contract term	Commencement Date until 31st March 2023
Possible extension periods	1st April 2023 – 31st March 2025

SECTION 2: Services Descriptions

The Supplier will be responsible for providing the 2nd and 3rd line ITSM capability, including operational management of 3rd parties, for the FCN X-Change, as specified herein. 1st line support will be provided by the Force IT Service Desk, who will pass on FCN Xchange tickets to the supplier following initial triage.

This service is likely to be extended to other national policing applications once those capabilities are developed and ready to be transitioned into live technical service and support, which will be covered by Change Control if applicable. These additional capabilities will follow the service model established and described within this document.

2.1 Service Model Overview

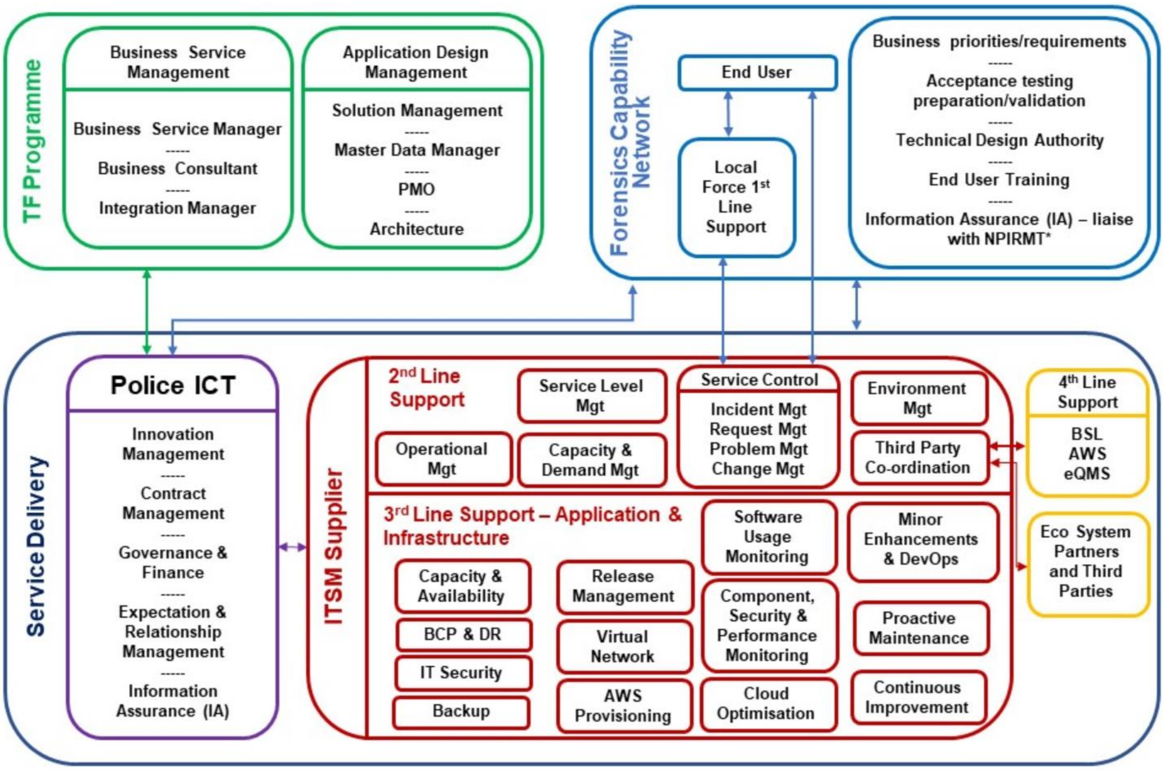
The FCN Xchange system is hosted on AWS cloud and developed by a 3rd party supplier under the management of the TF Programme. TF will continue to manage enhancements to the FCN Xchange system and introduce further forensics functionality. The Forensics Capability Network provide business support to users of the FCN Xchange system and over time will take over specific responsibilities from TF. They are the business user and client for the Service Delivery of the FCN Xchange system.

All 1st line calls will be delivered through the local Force IT function for triage, and if determined to be a fault or query with FCN Xchange will be handed over (via agreed process and tools) to the Service Delivery function. 1st line Police Force Service Desk will be contacted by end users directly where required, to progress investigation, triage or resolution of cases. Where required, the Supplier will also have the ability to directly contact users for further information to resolve a case. Where suitable, FCN, as the customer, may raise FCN related tickets directly with the Supplier using their Service Management tools, rather than from a force 1st line perspective.

The Service Delivery function is managed through the Company, and any escalations, contracts and interactions with FCN will be directly through the Company. User support will be provided by the Supplier, supporting 2nd and 3rd line capabilities for both infrastructure and applications, following standard ITILv3 processes, including operational management of 3rd parties, with underpinning contracts to 4th Line and other 3rd parties suppliers sitting with the Company.

On Day 1 of service, there will be limited interfaces to external systems, but these will be implemented at a date to be determined as future releases.

Depicted below is the target Service Model including the management of interfaces that will be implemented over the initial releases of FCN Xchange system.



2.2 In Scope Activities:

2.2.1 Set-up, Implementation, Knowledge Transfer & Transition

Prior to delivery of the services in this document, the Supplier will establish the Service Delivery function and deliver all requirements of the Transition Plan as part of Service Transition, within a timeline agreed with the Company, but in all cases by 1st November 2020. Within the timeframe specified within the Order Form, the Supplier shall provide the detailed Transition Plan and definition of deliverables to ensure a successful implementation of the ITSM capability.

The Supplier shall detail the following, as a minimum, within the Transition Plan:

- Transition objectives & methodology (including but not limited to onboarding of users and services) & management of the project activities, detailing requirements of all partners including Supplier, the Company, 3rd party suppliers and TF Programme to be delivered as part of the transition, to ensure end to end set up of the service
- Project governance for the duration of the Transition detailing updates, blockers to progress, risks and issues on all workstream activities, including items related to impact on Financial and Contractual workstreams

- Establishment of BAU governance reviews, agreement of Terms of Reference, and interaction with the Customer and the Company through jointly agreed processes and policies
- Technology requirements to enable the solution, including all workspace requirements are in place, and all technology, including correct security prior to the commencement of service
- Detailed Knowledge Transfer (KT) requirements, scope and monitoring procedures (in conjunction with the Company and Programme on scope)
- Qualified personnel to undertake the KT and to deliver the service
- The Supplier will provide a redacted copy of the final Call Off Contract documentation within 30 days of Call Off Commencement to enable the Customer to publish without release of commercially sensitive data.
- Develop a Service Design relevant to the service and support requirements, and implementation of the FCN Xchange
- Setup of Service, Operations processes, and tooling to provide the ITSM services during the contracted timeframe:

The Supplier shall not be permitted to take on the live service until the above requirements have been fully delivered and accepted as complete to the satisfaction of the Company and the Customer.

2.2.2 Service Management

A Supplier Service Manager will be appointed by the Supplier who will oversee all aspects of delivery of the services including but not limited to reporting, service review management, service delivery against the Service Level Agreements (SLA's) and Key Performance Indicators (KPI's), forthcoming projects and service outage plans, service delivery and trends, escalations for operational issues and be the single point of contact (SPOC) for queries and requests.

The Supplier and the Company will hold a monthly service meeting, as a minimum attended by the Supplier Service Manager and the Company Service Manager, which shall be face to face where possible at the Customer's premises.

The Supplier will provide a Service Management function across all services provided for the FCN Xchange, in accordance with the ITILv3 IT Service Framework (processes and tools). This includes accountability for services within their domain, and input into externally managed processes and policies (such as Data Protection Policies) where required.

This will be delivered through the Supplier's ITILv3 compliant ITSM toolset, consistent with Industry standard best practices. The tool will be integrated with the tools of other suppliers and customers, for which APIs need to be available and automation sought as best practice.

The Supplier must provide the following methods of communications to support Customer interactions:

- A web-based portal, that allows users to create, view and monitor ticket progress, capable of being branded in accordance with the customers' requirements
- a centralised email address such as "FCNXchangeSupport@supplier.com" and
- manned telephone help desk (local call cost).

The requirements for this Service include the following:

1. Service Control – Incident, Problem, Request and Change Management
2. Service Catalogue Management
3. Continuous Service Improvements: Strategic, Operational and Tactical
4. Capacity and Availability Management
5. Configuration Management
6. Software Asset Management, including usage monitoring, reporting, renewals management and audit
7. Service Level Management and Reporting through regular Governance
8. MI Reports - Dashboard, Reports, projections, Cost analysis
9. Management and resolution of support tickets
10. Management and execution of operational, remedial and emergency support and maintenance
11. Data backup and storage
12. Password Resets
13. Customer onboarding (account set up based on roles and prior approval)
14. Customer Satisfaction Monitoring and Reporting Liaison with the business and customers
15. IT Security Management.

2.2.3 3rd Party Suppliers Operational Management

The Supplier should recognise the importance of maintaining capability and capacity within the broader Supply Chain in order to ensure longer term support to the evolution of the FCN Xchange system. To this end, the Supplier must support the Company adoption of a 'multi-sourcing' approach to supply chain management which will involve the Company maintaining an 'Eco-System' of high-calibre suppliers across the IT development spectrum. The Supplier will support this approach by retaining operational responsibility for the delivery of support services as described within this document. The Supplier will also on-board and support development activity provided by other 'Eco-System' suppliers. The Company will contract directly with these 3rd Party Suppliers and shall procure that they co-operate accordingly with the Supplier, in line with a collaboration agreement, to which all parties shall agree.

The Supplier shall provide the following as part of this Service:

- Day to day logging of tickets to 3rd parties (where required), initially AWS, extant development partner and envisaged to be a further 6 Eco-System suppliers plus other technology vendors
- Support interfaces to other national police programmes e.g. HOB, BSG as required
- Management of ticket resolution including liaison and escalation within the 3rd party where required
- Escalation within the ITSM model for non-performance of the 3rd party
- Contractual escalation to the Company.

2.2.4 Major Incident Management

The Supplier will implement a Major Incident Management process to ensure the Customer (and other stakeholders as appropriate) are always kept up to date with all P1 and P2 severity incidents. For each Major Incident (MI) the Supplier will appoint a Major Incident Manager who will be accountable for the MIM process and own the MI for the FCN Xchange life-cycle.

The Supplier will provide the following services as part of this requirement:

- Define, refine, analyse, qualify and maintain the invocation of the Major Incident Management process
- Communicate and escalate as appropriate to predefined contacts, in and out of core hours
- As required, the engagement of a recovery Major Incident Team (MIT), consisting of Recovery Managers (RM), who will be responsible for the resolution management efforts of the major incident
- Ensure appropriately skilled resources are assigned to the resolving MIT to speed up the recovery process and minimise impact
- Develop, in conjunction with the RMs, an agreed resolution to the Incident in a timely and controlled manner to minimise impact to the customer
- Review of available information sources (e.g. managed Changes) to quickly identify the cause of a major incident
- Proactively manage, as required, resolution and escalation conference calls/bridges to facilitate timely resolution in alignment with the FCN BC/DR plan.

2.2.5 Support and Maintenance of the Amazon Web Services (AWS) Platform

The Supplier will administer, maintain and support the Company's AWS cloud computing platform for the FCN Xchange which includes the following:

- AWS – Active Directory
- AWS – Exchange Connectors
- Cloud Optimisation

- Cost / Spend Optimisation
- Component Monitoring
- Proactive Maintenance
- Performance Management
- Virtual Network
- Backup in AWS

Underpinning contracts with AWS will align with the agreed service levels particularly for the production environment, as per the standard offerings from AWS available from https://aws.amazon.com/premiumsupport/plans/

The Supplier must follow and adhere to the National Cyber Security Centre (NCSC) Cloud Security Principles and will be audited against such requirements to demonstrate compliance alongside implementing recommendations from AWS Well architected reviews.

2.2.6 Software Application Support

The Supplier will provide support and maintenance (including bug fix) throughout the contract to mitigate product obsolescence risks and ensure it continues to deliver value to Policing, through administration and end-user support for the FCN Xchange software applications.

This includes the following:

- Software usage monitoring and reporting for all components of the FCN Xchange
- Maintain application updates and minor enhancements via DevSecOps
- Asset management of software using the Supplier Configuration Management Database (CMDB)
- Performance Management of the Application
- Audit Services where required
- Access Management & Release to new force personnel
- Environment management across the ecosystem including data refresh where required
- Via the individual Forces 1st line service desk, or FCN, support and resolve end users with any tickets raised in relation to their software applications including liaison with suppliers & customers where required.

2.2.7 Development, Enhancements & Release Process

Working in line with OWASP, NIST and NCSC recommended best practice, the ITSM capability to be established by the Supplier must be flexible and scalable to cater for the incremental on-boarding of supplement capability and capacity throughout the life of the contract. The initial FCN Xchange system incorporates specific functionality and will be known as "Release 1" however the Supplier will support the dynamic product enhancement environment which is envisaged.

The Supplier will therefore, at no extra cost, provide support and deployment to the following release profile post-Release 1 as part of their Service Introduction capability:

- Minor developments e.g. bug fixes: approximately 1-2 every month
- Major enhancements to existing capability, e.g. fingerprint capability integration with HOB or National IAMS or NMC approximately 1 every 3 months
- Major Change: introduction of significant new capability, such as digital forensics or a new COTS product: approximately every 3-6 months, in turn comprising of a number of releases. This will typically be managed as a new Project.

The Supplier must retain sufficient capacity and capability within its organisation to support the above release cycle. To support this requirement, the Company will provide an updated technical roadmap on a 6-monthly basis, on an 'information-only' basis.

Any enhancements or new functionality to the delivered capability will be developed and deployed following approved change request procedure and in line with Industry best-practice release and configuration management practices. Change Control will be implemented to support the DevSecOps process to ensure alignment of release, enhancement and production environments.

New applications developed for other Forensics services (DNA, workflow etc.) will follow their own development and production deployment paths but will follow the standard change control and agreed Operational Acceptance Criteria before coming into service.

This is intended to be a flexible and agile approach that will allow FCN and the Company to satisfy the future capability and capacity requirements in a modular and efficient method that provides value for money through-life.

2.2.8 IT Security

The Supplier will provide IT Information and Security Management services for the software applications in line with OWASP, NIST, NCSC, and NPIRMT best practice. This includes the following:

- Compliant with the Security Aspects Letter (SAL) provided as attached to the Order Form

- The service being provided by the Supplier must be certified to ISO27001
- All supplier staff who access police information must be NPPV3 Cleared by the National Contractor Vetting Scheme - Warwickshire Police (unless, at the Customer's discretion, a temporary waiver is granted that allows staff with SC clearance to be utilised in delivering the services)
- Within 90 days of Commencement date, the Supplier will provide an audited IT Health Check (ITHC) report (provided by a separate 3rd party CHECK supplier) of their Service Management and monitoring system. For both their own and FCN Xchange system, it is a requirement to annually provide an updated ITHC report dated within the previous 12 months, detailing findings and a mitigation plan against findings
- The Supplier will provide, at no additional cost, an annual IT Healthcheck or upon major system changes
- Patch Management
- Monitoring of security alerts
- Threat and Vulnerability Management of all environments
- Comprehensive Logging and Protective Monitoring (including CSI activities for audit purposes)
- Management of Security Tooling including: Intrusion Detection System (IDS) / Intrusion Prevention System (IPS), Firewalls, Antivirus / Anti-bot / Anti-spam, URL Filtering
- Infrastructure (AWS) and Application Level Security Controls
- Code reviews of any development work prior to implementation into the production environment
- Encryption Key Management & Implementation
- Network Address Translation (NAT) and Proxies
- Penetration testing and code reviews that are non-CHECK certified on a quarterly basis
- Data retention and deletion in line with FCN requirements.

In the near future, on a date to be determined, NEP Identity & Access Management (IAM) and the National Management Centre (NMC) for Policing will be enabling a standard security monitoring solution across national police forces, including the FCN capability. The Supplier will need to interact as an additional 3rd party with these organisations.

2.2.9 Change Management

All change requests will be logged by the Supplier within the Supplier service portal. Changes will be processed according to the Change Control Procedure with a planned maintenance notice for the work to be carried out by the Supplier or any 3rd party provider. All changes are subject to the agreed Change Control Procedure.

Change Requests should be categorised according to the following table and will be actioned in accordance with the KPI shown in this document.

Change Request Categorisation	
Priority	**Incident Type**
Normal	This covers most requests for a change to a system that require CAB approval due to a change to a [CI] or from the request fulfilment process. Change Control Procedure to be followed.
Standard	This is a change that has already had the repeatable process approved by CAB and therefore does not require further CAB approval or a new RFC, provided this is expressly stated on the original Change Authorisation Note (as defined within the Company Service Delivery Framework document). A list of standard RFCs will be updated for reference as new, minor changes, are approved at CAB e.g. adding a firewall rule, an RFC is required as the [CI] change needs tracking. However, after an RFC has been approved future changes simply require a RFC with the specific details of this change and linked to the initially approved Change Authorisation Note. Only to apply to changes expressly approved in the initially approved Change Authorisation Note
Emergency	A change needed to help resolve an emergency incident. Due to the urgency of the change it may not go through CAB but instead go through an emergency approval from the Head of Service Management or senior management. This approval may be verbal provided it is follow-up in an email within one Working Day. However, once the incident is resolved a retrospective RFC needs to be completed and logged.

2.2.10 Business Continuity and Disaster Recover (BCDR) Invocation Services

The Supplier shall provide, within the timescale specified in the Order Form, a completed Business Continuity and Disaster Recovery Plan detailing the levels of failures and disruptions to the services and the subsequent business processes and operations that the Supplier will invoke (including roles & responsibilities) to ensure the continuity of the ITSM service following any failure or disruption to the ITSM element of the FCN Xchange. The plans must also demonstrate the impact that invocation may have on the operation of the service, ensuring continuity of business operations during any period of service failure or disruption, with, as reasonably practicable, minimal adverse impact to the services being supported. These plans will be subject to review by the Company and once accepted by the Company, will form part of the overarching FCN Xchange BCP/DR plan(s**).**

In the event of a complete loss of service or in the event of a Disaster, the Supplier shall immediately invoke the BCDR Plan (and shall inform the Company promptly of such invocation). In all other instances the Supplier shall invoke or test the BCDR Plan only with the prior consent of the Company.

The Supplier will action and follow agreed procedures and processes relating to the invocation of BCDR services as part of the overarching FCN Xchange BCDR plan(s). Should an invocation be requested the Supplier Account Manager will be responsible for communication to the Customer Service Delivery Manager. The Supplier will recover the systems and infrastructure in line with the Disaster Recovery Plan.

The Supplier will review the BCDR plans on a regular basis and at a minimum every 6 months, to ensure that they reflect the current requirements of the FCN Xchange.

2.2.11 Business Continuity and Disaster Recovery Exercises

The Supplier and the Company will agree a scope of work detailing the frequency and scale for BCDR exercises to be performed over a 12-month period. This will include both desk top and real-time exercises and will include at least 1 major exercise per 12-month period. Agreed success criteria will be established to determine whether the exercises achieved the objectives. Supplier will appoint an observer to monitor the BCDR exercises, to record any actions and ensure the BCDR plans are followed in accordance to the documented procedures. The Supplier will provide technical personnel to work with the Company to recover the systems in line with the agreed procedures. A post exercise review will be performed with the Supplier and the Company will report against the defined success criteria and to ensure that any captured actions have appropriate owners and are established with a defined timescale for delivery. The response should include how the Supplier will ensure the FCN services will be brought online minimising the impact any incident has. It should also detail how the Supplier will meet FCN Recovery Time Objective (RTO) and Recovery Point Objective (RPO) that will be defined by FCN.

2.2.12 Exit Management

Prior to completion of the delivery of the services in this document, or at a mutually agreed end date, the Supplier will hand over the delivery function to a new ITSM Supplier, to be completed within a timeline agreed with the Company. The Supplier will provide details around the methodology they will utilise to perform this transfer. On commencement of the Exit, the Supplier shall provide the detailed plan and deliverables to ensure a successful handover of the service from the current Supplier, into the new Supplier ITSM function. This will require full management of the handover from the Supplier perspective, to ensure end to end handover of the service, without impacting on the day to day delivery of the service:

- Project governance for the duration of the Exit, detailing updates, blockers to progress, risks and issues on all workstream activities, including items related to impact on Financial and Contractual workstreams
- Technology overview of the solution, including correct security access prior to the commencement of service from the new Supplier
- Detailed Knowledge Transfer (KT) requirements and scope
- Qualified personnel to undertake the KT to the new Supplier
- Handover of Service, Operations processes, tooling and associated Service design
- Deletion of data from Supplier systems (RG), signed off and assured against NCSC guidance on Security Sanitation of Storage Media.

2.3 Service Hours

The service shall include contracted hours of “Service Desk” availability to support end users during the Company’s business hours. The service shall also include a provision of emergency out of hours support for Priority 1, cyber and security incidents. The availability hours are as follows:

Availability Hours			
	Days of Operation	Hours of Operation	Communication Method
Contracted Hours of Support	Monday to Friday	7am to 10pm	Telephone, Email and portal
Out of Hours Support	Monday to Sunday	24 Hours (excluding contracted hours)	On Call Telephone Only

All tickets logged via the Service desk will be categorised using the following:

Service Ticket Categorisation

	Definition	Initial Response	Resolution	Feedback Intervals
		In Business Hours		
Priority 1 (P1)	An outage or issue affecting all users	Within 30 Minutes	4 hours	Hourly
Priority 2 (P2)	A partial outage or issue affecting multiple users or an outage affecting all users with a workaround	1 hour	8 hours	2 hours
Priority 3 (P3)	An outage or issue affecting a single user	4 hours	24 hours	8 hours
Priority 4 (P4)	No service affecting	8 hours	48 hours	24 hours
Service Requests (SR)	User requests for information or advice, or for a standard change (a pre-approved change that is low risk, relatively common and follows a procedure) or for access to an IT service – for example a password reset	*Telephone: Instant* *All other forms:* *4 hours*	*As per Service Catalogue*	*8 hours*
Non Standard Service Request (NSR)	Need for an adjustment of a system or application. That has been pre-approved as a standard change.	8 hours	As per quote	8 hours
Known Error	A problem which has a documented root cause and a workaround	n/a	n/a	Service Meetings
Problem	The cause of one or more incidents which requires an RCA and has no workaround	n/a	24 hours	Service Meetings

2.4 Governance & Service Reporting

The Supplier will support a governance model which will be established to ensure appropriate operational service management and strategic alignment between all stakeholders. This 2-tier governance framework will be established and Terms of Reference agreed during the Transition phase.

The Governance model will consist of the following:

<u>Strategic level</u>

- Determine business strategy

- Provide senior level guidance and leadership for the overall delivery
- Ensure that contractual agreements are operated throughout the term in a manner which optimises the value for money and operational benefit
- Deal with major operational disputes and events
- Notified in instances of a MI and progress towards resolution.

Operational level

- Attended by operational level managers and other personnel as required
- Forum for dealing with day to day operational management issues
- Managed of MI instances
- Raise Issues and Risks with the service
- Prioritisation of work activities.

Monthly Operational Service Review: To review the provision of the services delivered by the Supplier to the Company against the agreed KPI measures, as well as being an opportunity to discuss and provide update on any relevant current or upcoming activities being undertaken by each organization. The Supplier will provide a series of reports monitoring the services for a monthly period by the 10th of the following calendar month (or nearest working day). The report will include data from the current, and prior 6 months of service, where this data is available. Access to source data should be made available to the Company for assurance purposes.

The following data will be made available to the Company 3 business days before the monthly service meeting is being held:

Service Management Reports	
Report	**Minimum Included:**
Incidents	a) Number of incidents raised a. How was the ticket raised – email, phone, portal b) Number of current open incidents a. Age of oldest incident b. Incidents over 7 days c) Categorisation of incidents d) Number of incidents re-opened e) Percentage of incidents resolved at first call (via 2nd line escalation) f) Any identified trends g) Average time to resolve – identification of any incidents breaching SLA h) Number of additions to knowledge base (for quicker incident resolution in the future) i) Identify any service improvements

	j) Number of current problem tickets, number new this month, number closed and number over 14 days k) Number of known errors, number of new this month and number closed l) Security Incidents
Service Request	a) Number of standard SRs complete in the period b) Number of non-standard SRs complete in the period c) Number of SRs open a. Age of each open SR b. SRs over 7 days d) Average time to complete standard / non-standard SRs
Change Requests	a) Number of changes by type complete in the period b) Number of successful and failed changes complete in the period, with analysis of failures
Monitoring and Alerts	a) Health and availability of critical infrastructure and application components and services b) Alerts have been generated and the investigation and actions taken by the service desk c) Vulnerabilities and threats reporting, and actions taken d) Patching status across all services
Risks and Issues	a) Should Identify any key risks / issue, change from last report
Financial Reporting	a) Provide invoicing data in line with the agreed financial process, ensuring accuracy of data contained within, to facilitate approval and payment of in a timely manner

Note: These reports monitor specific services as requested by the Company, these are in addition to monitoring of SLAs and KPIs which is outlined in Section 3. Operational reporting will also be required in order to manage the service.

Strategic Review: To provide a forum for senior representatives from the Company, the Supplier and other key stakeholders invited at the discretion of the Company as appropriate e.g. FCN leadership, to review overall performance and set the strategic direction for the relationship with the Supplier. The meeting will examine key opportunities and threats to future performance and serve as a point of escalation for any issues that cannot be resolved through other forums. This meeting is held quarterly and is attended by the respective leadership teams of each organization at the Company’s premises.

2.5 Out of Scope

Although not an exhaustive list, below are some elements of the not required to be delivered by the Supplier. By default, if an activity is not specific to the FCN Xchange solution it is not in scope:

- Core FCN Business Service Desk support
- Provision of 1st Line support
- Provision and support of all end user devices and hardware (e.g. laptops, mobile phones, cameras etc), supported through existing channels

- Costs for AWS platform consumption
- The Supplier is not required to perform any integration activity for the police force(s) users EXCEPT that they are able to use the IT services offered by FCN
- Each police force will be responsible for the provision of Local Area Network (LAN), Wi-Fi and Wide Area Networks (WAN) and support there of
- Support for Customer corporate systems e.g. Finance, Procurement & Legal (Enterprise ERP Systems), Back Office tools

SECTION 3: Managing SLAs and KPIs

Sections 4 and 5 to this Document set out the Service Levels and KPIs which the Parties have agreed to measure in respect of the Suppliers performance of the Services.

The Supplier shall monitor its performance in delivering the Services against the Service Levels and KPIs and shall send the Company a monthly report detailing the level of service which was achieved against these measurements as detailed above.

The principle underlying the SLAs and KPIs is that they provide a mechanism for the Company to measure the quality of service received from the Supplier and to incentivise the Supplier to maintain that quality of service. The intention of the Service Levels and Key Performance Indicators is not to penalise the Supplier for incidents that are outside of the Supplier’s control or those cannot reasonably be planned for or prevented.

3.1 Service Reviews and Failures

The Parties shall conduct service reviews in respect of the performance of the Services by the Supplier under this Agreement (each a “**Service Review**”). The frequency and extent of Service Reviews shall be agreed by the Parties and shall be in proportion to the scope of Services provided. Service Reviews will consist of virtual conference or site visits at the agreement of both Parties.

The Supplier shall report on any Service Failures at the next Service Review In the event of a High Severity (P1 or P2) incident (as defined herein), and an interim incident summary will be provided within three Working Days of resolution. The Parties shall use the Service Review as an opportunity to discuss the root cause of the relevant Service Failures (if any) and actions the Supplier will take to achieve the relevant Service Levels and/or KPI in the future.

3.2 Service Availability

Services will be available 00:00 to 24:00 Monday to Sunday, including statutory holidays, with the exception of scheduled and emergency maintenance (as defined below). Support hours of the services are detailed in the "Support Hours" section.

All scheduled maintenance in line with associated Services shall be completed outside of 07:00-22:00 ("Core Business Hours") and advance written notification of such work shall be provided to the Company by the Supplier at least 5 Working Days in advance ("**Permitted Downtime**"). A change calendar should be provided looking forward for 12 months, with preapproved maintenance windows in line with known change blackout dates provided by the Company

Wherever possible emergency maintenance will be completed outside of Core Business Hours. Advance notification of such work shall be provided to the Company by the Supplier prior to commencing in line with agreed escalation procedures.

Note: Emergency maintenance is defined as urgent unscheduled maintenance necessary to avoid an imminent threat to the infrastructure, network or the Company's assets.

To the extent that the Service Levels set out in Section 5 of this SLA relate to uptime of particular Services ("**Service Uptime**"), such Service Uptime shall be calculated in accordance with the following formula and rounded to two (2) decimal places, to determine the uptime of that infrastructure during the relevant time period (as described in the relevant SLA) per calendar month ("**Relevant Period**"):

Service Uptime % =

$$(MP - SD) \times 100 / MP$$

where:

MP = total number of minutes within the Relevant Period

SD = total number of minutes in the Relevant Period when the relevant Service(s) is not operating, including such resolution time as is required to return the affected infrastructure / applications to operational service or escalate to the Company in line with agreed escalation procedures.

The following events shall be excluded from any assessment of Service Downtime:

- Permitted Downtime;

- Service Downtime resulting from emergency maintenance, in each case where the Supplier has taken steps to mitigate impact of downtime on the Company;
- Service Downtime due to interoperability issues between the Company applications or designs and the systems managed by the Supplier, provided that such issues are outside the scope of the Supplier's obligations under the Agreement;

Service Downtime due to failure of third party services used in the provision of the Services where such third-party services are outside the scope of the Suppliers' obligations under this Agreement (except to the extent such failure arises from the Suppliers' failure to comply with its obligations under this Agreement).

SECTION 4: Service Level Agreement

4.1 Introduction

This section sets out the Service Measures, which must be met by the Supplier in performing the Services in accordance with agreed procedures. The Key Performance Indicators (“**KPIs**”) and Service Level Agreements (“SLAs” form part of the agreement between the Company and The Supplier of the level of service that is expected on a day-to-day basis for all users.

SLAs detail where Service Credits are applicable should the Supplier fail to provide the Services to meet them. Consistent failure in KPIs could also result in Service Credits being applied.

Prior to Service Credits being applied, data must be gathered by the Supplier for 3 months to validate assumptions on volumes, and performance against targets to ensure they are applicable to the live service. Post this baselining period service credits will be immediately applicable against validated targets.

Baseline Approach

Figure 1 below describes the process involved in the development of the service baseline:

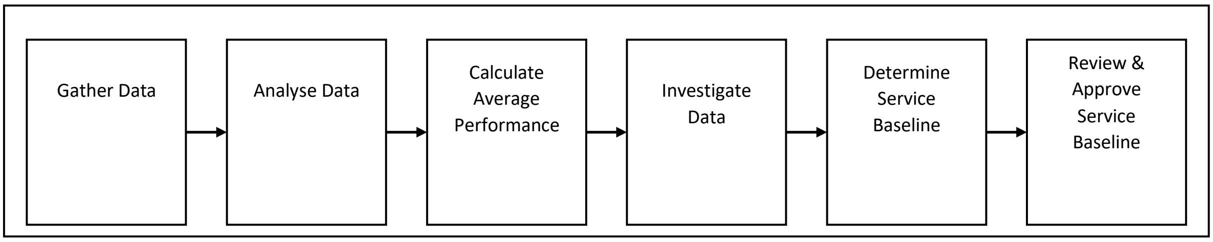

Gather Data
Analyse Data
Calculate Average Performance
Investigate Data
Determine Service Baseline
Review & Approve Service Baseline

Figure 1 - Service Baseline Process

- Gather Data: Service measured data is gathered for three months from support Go-Live (~90 days).

- Analyse Data: A detailed review of baseline trends is conducted to determine whether during the baseline period the data is an accurate reflection of the services provided.
- Calculate Average Performance: The average performance over the three months period is calculated.
- Investigate Data: Explanations are sought for baseline trend fluctuations. Once the variations have been explained, appropriate agreed adjustments may be made to the baselines during the data collection period.
- Determine Service Baseline: The service baseline is set. The chosen approach to determining the baselines from the existing data is to calculate the average performance where appropriate. In cases where an anomalous result has occurred, it may be omitted from this figure, with an explanation for this in the comments. (e.g. spikes caused by product releases).
- Review and Approve Service Baseline: The baseline is then reviewed and approved.

Measure	SLA / KPI	Target	Minimum
Minor Enhancement Management			
Percentage Work Efforts on Budget*	SLA	90%	85%
Percentage Work Efforts on Document*	SLA	90%	85%
Budget Variance at Completion	KPI	90%	85%
Document Variance at Completion	KPI	90%	85%
Incident Management			
Backlog Processing Efficiency-Incidents (Priority 1-4)	KPI	100%	90%
Percent Resolved Incidents Reopened	KPI	0%	2%
Resolution Time Performance - Incidents (Priority 1-4) *	SLA	95%	90%
Response Time Performance - Incidents (Priority 1-4) *	KPI	100%	95%
Application Availability	SLA	100%	98%
Problem Management			
Backlog Processing Efficiency - Problems (Priority 1-4)	KPI	100%	90%
Root Cause Analysis Completed on Time	KPI	100%	90%
Change Management			
Number of Failed Changes	SLA	0%	2%
Number of Changes Completed Late	SLA	0%	2%
Quality Management			
Defect Closure Trend	KPI	<25%	<20%
Fix Backlog Trend	KPI	>10%	>5%
Peer Review Effectiveness	KPI	90%	80%

Testing Effectiveness	KPI	95%	90%
Requirements Management			
Change Request Impact	KPI	0%	2%
SLA Performance			
Percent SLAs Met*	SLA	100%	90%
Percent KPIs Met*	SLA	80%	75%
Platform is kept in step with Government cloud agenda including NPIRMT, NCSC guidance and controls	KPI	Within 1 month of changes	Within 2 months of changes

Annex 1: Technical Specification

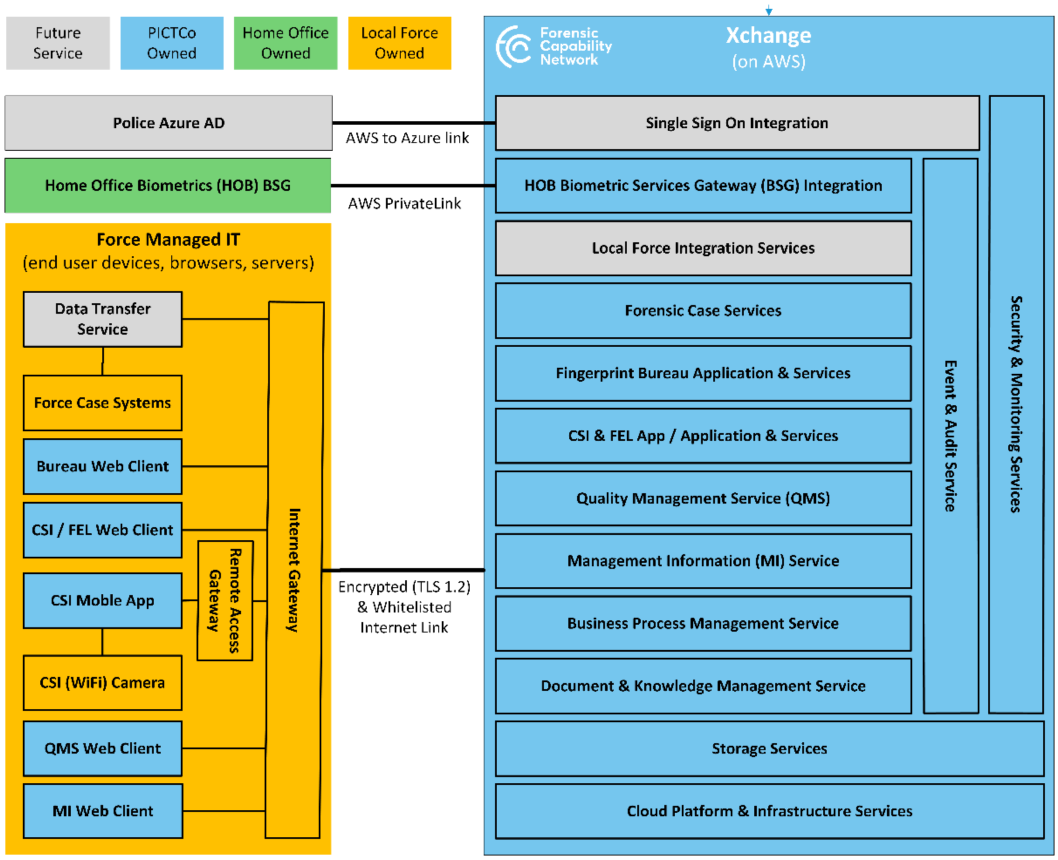
To support the forensic community and delivery on the objectives of the Forensic Capability Network, the Transforming Forensics programme has developed the Xchange platform and services. Xchange is an AWS cloud-hosted platform that provides a set of capabilities, such as storage of crime scene images, to support Web-based applications and an Android mobile app, designed for specific forensic users. The capabilities of the Xchange platform and services include:

- A mobile app to mark-up and transfer digital images from the crime scene.
- Central storage and management of scene photos and associated metadata.
- Integration with police systems, starting with IDENT1.
- Web-based services for Fingerprint Practitioners to compare marks to tenprints.
- Workflow and tasking to guide Bureau staff through examinations.
- Management Information and dashboards for Forensic Service Managers.
- Audit of all user and system activity to monitor compliance to legal requirements and forensic ISO standards.
- A Quality Management System (QMS) to:
  - Store and control quality documents, such as Standard Operating Procedures (SOPs) and validations.
  - Allow staff to log non-conformances and track activity to rectify.
  - Run other quality procedures, such as scheduled checks of equipment.

TF also plans to extend Xchange in the future to include:

- Integration with Azure-based Single Sign On – as designed by NEP and to be run by the Police ICT Company.
- Integration services to share data with local force systems, such as criminal case management systems.

The diagram below illustrates the solution and key integrations with all planned services, i.e. initial releases and planned near term work:


Future Service
PICTCo Owned
Home Office Owned
Local Force Owned
Forensic Capability Network
Xchange
(on AWS)
Police Azure AD
AWS to Azure link
Home Office Biometrics (HOB) BSG
AWS PrivateLink
Force Managed IT
(end user devices, browsers, servers)
Data Transfer Service
Force Case Systems
Bureau Web Client
CSI / FEL Web Client
CSI Mobile App
CSI (WiFi) Camera
QMS Web Client
MI Web Client
Remote Access Gateway
Internet Gateway
Encrypted (TLS 1.2) & Whitelisted Internet Link
Single Sign On Integration
HOB Biometric Services Gateway (BSG) Integration
Local Force Integration Services
Forensic Case Services
Fingerprint Bureau Application & Services
CSI & FEL App / Application & Services
Quality Management Service (QMS)
Management Information (MI) Service
Business Process Management Service
Document & Knowledge Management Service
Event & Audit Service
Security & Monitoring Services
Storage Services
Cloud Platform & Infrastructure Services

Longer term, Xchange will be expanded to support further traditional 'wet' forensic and digital forensic processes and case management.

The Xchange platform needs to be resilient to the failure of any one component or service and provide high availability of the services, as it will play a critical role in forensic investigations. Use of cloud-native services and containerised deployment enables fully automated high availability across three AWS Availability Zones.

Further resilience is provided by ensuring all persistent data (evidence, case records, logs, etc.) is backed up. Lifecycle policies and versioning is also configured for AWS storage to ensure evidential integrity and retention policy compliance.

The information managed within Xchange is designated OFFICIAL-SENSITIVE HIGH. Xchange is designed to provide both security at the perimeter of the platform, as well as security-in-depth within. Operational services will run from the Production environment, within a separate security account and Virtual Private Cloud (VPC). As the business data will reside in this environment, it will be protected from all but required access, both internally within the Police Forces and from the outside World. Business user interaction will be via a separate Edge VPC over a locked-down API with controls such as IP whitelisting and TLS 1.2 encryption.

Authentication and access control is applied throughout using integrated Identity and Access Management technology. A ‘zero-trust’ policy is enforced so that internal services require other components to authenticate and communicate over encrypted channels.

Xchange microservices and applications are deployed in containers within a managed container orchestration environment, with further controls enforced by a service mesh. This approach greatly limits what containers can do, for example applying fine-grained access control on which services each container can user. It also allows for uniform security policy and network controls to be applied, for example enforcing TLS authentication and encryption of communication between microservices.

Xchange is built, and will need to be managed, using best practices of Secure DevOps that include:

- Building all environments from software-defined infrastructure using proven and tested pipelines and code.
- Using automation to guarantee immutable builds, i.e. only making direct config changes in extreme circumstances.
- Extensive security checks in the build phase to shift assurance and compliance left, for example with continually scanning to inspect the composition of all containers for vulnerabilities or breaches of security policies.
- Continual update of threat databases and known vulnerabilities, to apply to builds but also in intrusion detection and protective monitoring of the operational system.
- Security-in-depth as a fundamental design principle, and alignment with best practice, including National Cyber Security Centre (NCSC) cloud security principles and AWS Security Best Practices.
- Comprehensive monitoring, logging, and alerting.
- Continuous improvement of the above, automating wherever possible, and using the componentised / microservice architecture to replace technology with better / more secure alternatives as they become available.

The rapid build and deployment process, used to create new environments or patch existing ones, is illustrated below:

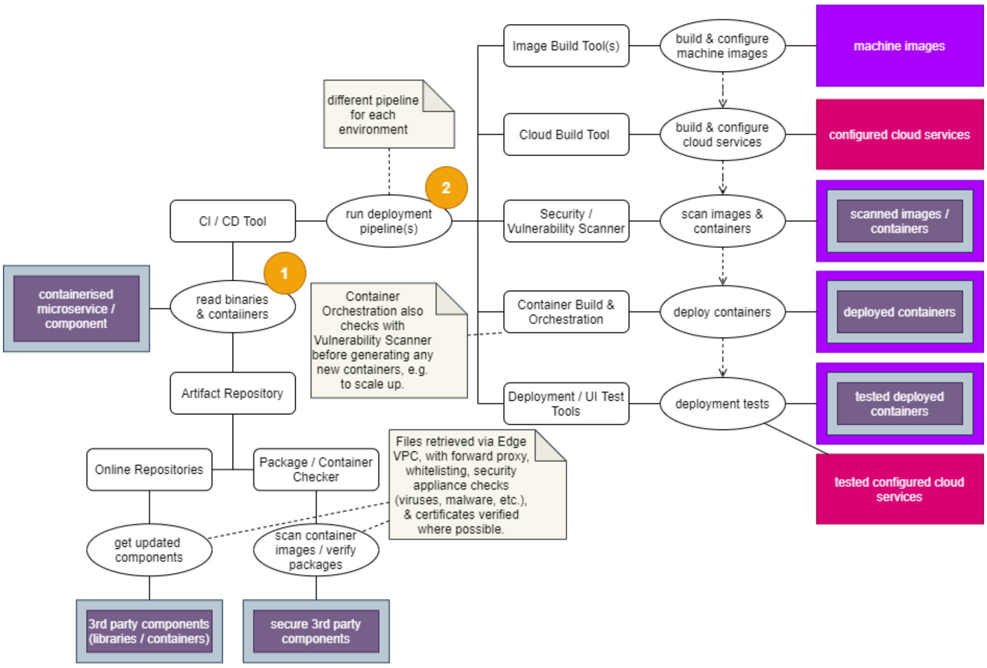
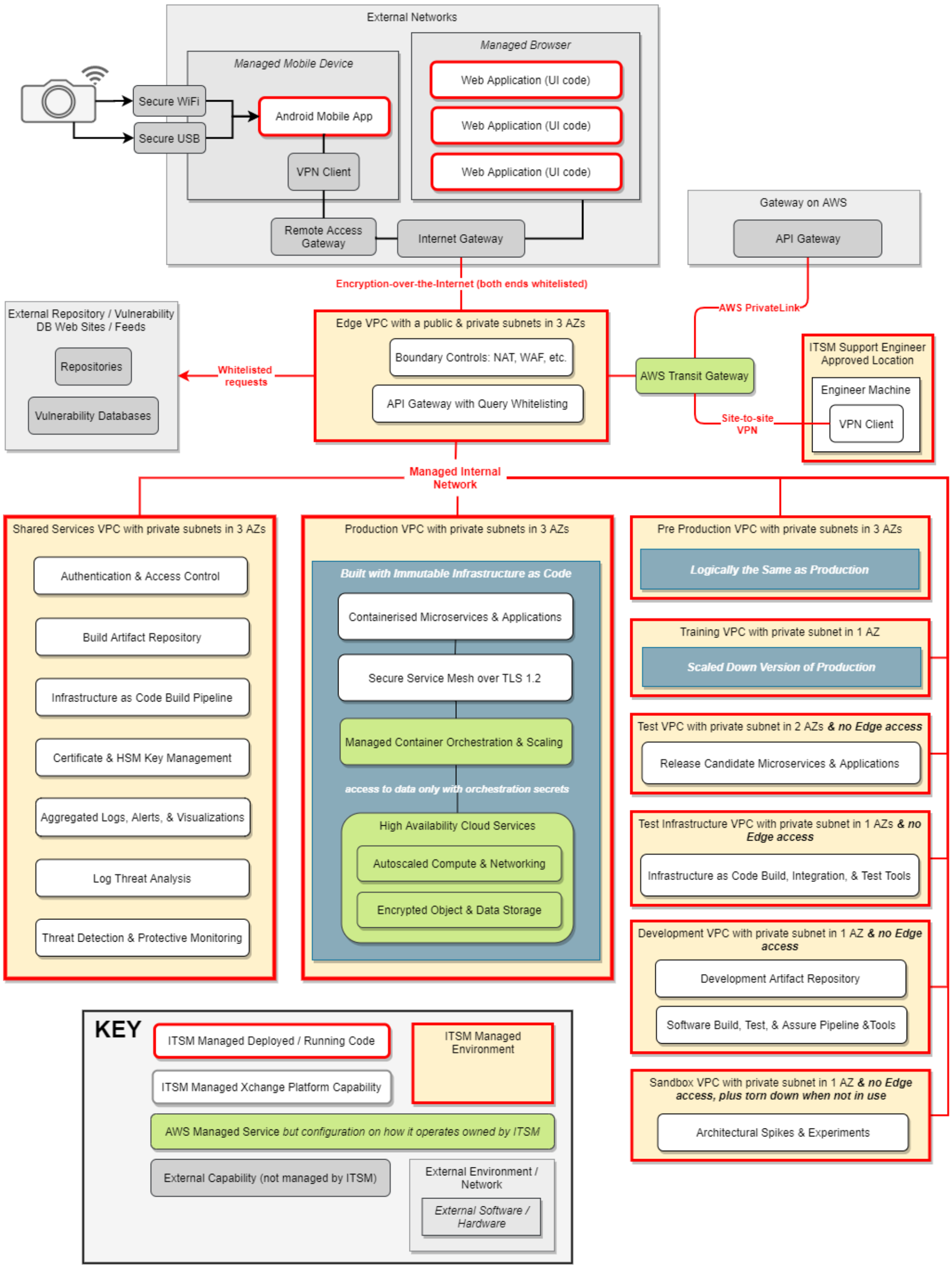


Image Build Tool(s)
build & configure machine images
machine images
different pipeline for each environment
Cloud Build Tool
build & configure cloud services
configured cloud services
2
CI / CD Tool
run deployment pipeline(s)
Security / Vulnerability Scanner
scan images & containers
scanned images / containers
1
containerised microservice / component
read binaries & contaiiners
Container Orchestration also checks with Vulnerability Scanner before generating any new containers, e.g. to scale up.
Container Build & Orchestration
deploy containers
deployed containers
Artifact Repository
Deployment / UI Test Tools
deployment tests
tested deployed containers
Files retrieved via Edge VPC, with forward proxy, whitelisting, security appliance checks (viruses, malware, etc.), & certificates verified where possible.
Online Repositories
Package / Container Checker
tested configured cloud services
get updated components
scan container images / verify packages
3rd party components (libraries / containers)
secure 3rd party components

The diagram below illustrates the different Xchange environments, the main components they will host, and the access between them and with external environments.


External Networks
Managed Mobile Device
Secure WiFi
Secure USB
Android Mobile App
VPN Client
Managed Browser
Web Application (UI code)
Web Application (UI code)
Web Application (UI code)
Remote Access Gateway
Internet Gateway
Gateway on AWS
API Gateway
Encryption-over-the-Internet (both ends whitelisted)
AWS PrivateLink
External Repository / Vulnerability DB Web Sites / Feeds
Repositories
Vulnerability Databases
Whitelisted requests
Edge VPC with a public & private subnets in 3 AZs
Boundary Controls: NAT, WAF, etc.
API Gateway with Query Whitelisting
AWS Transit Gateway
Site-to-site VPN
ITSM Support Engineer Approved Location
Engineer Machine
VPN Client
Managed Internal Network
Shared Services VPC with private subnets in 3 AZs
Authentication & Access Control
Build Artifact Repository
Infrastructure as Code Build Pipeline
Certificate & HSM Key Management
Aggregated Logs, Alerts, & Visualizations
Log Threat Analysis
Threat Detection & Protective Monitoring
Production VPC with private subnets in 3 AZs
Built with Immutable Infrastructure as Code
Containerised Microservices & Applications
Secure Service Mesh over TLS 1.2
Managed Container Orchestration & Scaling
access to data only with orchestration secrets
High Availability Cloud Services
Autoscaled Compute & Networking
Encrypted Object & Data Storage
Pre Production VPC with private subnets in 3 AZs
Logically the Same as Production
Training VPC with private subnet in 1 AZ
Scaled Down Version of Production
Test VPC with private subnet in 2 AZs & no Edge access
Release Candidate Microservices & Applications
Test Infrastructure VPC with private subnet in 1 AZs & no Edge access
Infrastructure as Code Build, Integration, & Test Tools
Development VPC with private subnet in 1 AZ & no Edge access
Development Artifact Repository
Software Build, Test, & Assure Pipeline &Tools
Sandbox VPC with private subnet in 1 AZ & no Edge access, plus torn down when not in use
Architectural Spikes & Experiments
KEY
ITSM Managed Deployed / Running Code
ITSM Managed Environment
ITSM Managed Xchange Platform Capability
AWS Managed Service but configuration on how it operates owned by ITSM
External Capability (not managed by ITSM)
External Environment / Network
External Software / Hardware

A number of DevOps tools and products are being utilised in the development of the FCN Xchange and as such, Suppliers must have the capability and capacity to support them accordingly. The following is not an exhaustive list but provides a summary of the kay products used at present:

Repositories

GitLab, Nexus OSS, RPM Package Manager (RPM), Maven, Docker Hub, gitlab.io, jenkins.io, mvnrepository.com, npmjs.com, RubyGems.org, PyPI

Quality and Security Inspection

Sonaqube, Quay.io, YUM, Anchore Enterprise, Kubeva, Hadolint, Sonarqube Community Edition

Build Tools

Jenkins, Ansible, Terraform, Packer, Kubernetes, Kubernetes Kind, Docker

Test Tools

Junit, Chef Inspec, pytest, Ranorex, Jmeter, Terragrunt, Kubetest, Molecule

Annex 2: Anticipated roll-out of FCN Xchange

The estimated % adoption of the national Fingerprint capability is outlined as follows for the roll-out to national police forces of the FCN Xchange:

On-boarding period	% of national Fingerprint capability	Cumulative	No. of Users
Oct-20	5%		94
Jan-21	7.5%	12.5%	141
Apr-21	20%	32.5%	375
Jul-21	20%	52.5%	375
Oct-21	20%	72.5%	375
Jan-22	10%	82.5%	188
Apr-22		82.5%	
Jul-22	10%	92.5%	188
Oct-22		92.5%	
Jan-23	7.5%	100%	141
Apr-23		100%	
	100%		1876

It should be noted however that each police force will undergo its own incremental on-boarding plan for staff. It is anticipated that each force will adopt the following on-boarding approach depending on each type of user:

Months from Force take-on of FCN Xchange	Bureau staff	CSI staff
Month 1	5%	5%
Month 2	75%	25%
Month 3	100%	90%
Month 4		95%
Month 5		100%

The information provided within this Annex is provided as an estimate only which the Customer reserves the right to amend accordingly as roll-out planning matures. The Customer fully expects the Supplier to support a flexible and incremental roll-out the FCN Xchange.