ICT Asset Management Plan

2020 - 2025

Table of Contents

ICT Asset Management Plan

1 Overview

1.1 Information and Communication Technology (ICT)

The Authority currently owns the ICT assets in the ICT infrastructure and the ICT applications that run on the ICT infrastructure. The ICT challenge is to provide the most functional, flexible ICT infrastructure possible, to host the applications that deliver benefits to the Authority, all at the lowest cost of ownership. Meeting this challenge systematically through having the right people in the right structure, Infrastructure Lifecycle Management (ILM), Application Lifecycle Management (ALM) and best practices, such as the Information Technology Infrastructure Library (ITIL) can lead to improvements in efficiency, performance and cost management.

ICT can be split into six key delivery areas:

- The ICT infrastructure - data network, voice and radio networks, personal computers (PCs) and devices, servers, printers, etc.
- Commodity applications which run on the ICT infrastructure – Structured Query Language (SQL), Oracle, Microsoft Office and e-mail
- Fire Control applications which run on the ICT infrastructure - Vision FX Computer Aided Dispatch (CAD), Vision FX BOSS, SEED and the Staff Attendance Recording System (S.t.A.R.S)
- Financial applications which run on the ICT infrastructure - ABS eFinancials and ResourceLink
- Corporate applications that run on the ICT infrastructure - Tranman, Planning Intelligence and Performance System (PIPS), the intranet 'portal', Simple Operational Fire Safety Assessment (SOFSA), Site Information Risk and Hazard (SIRAH) and Sophtlogic
- The ICT Service Desk - the central point of contact between ICT providers and users on a day-to-day basis. It is also a focal point for reporting *Incidents* (disruptions or potential disruptions in service availability or quality) and for users making *service requests* (routine requests for services)

The Authority has an in-house ICT team of staff ('ICT') which proactively manages the existing outsourced ICT managed service contract with its ICT partner, telent. ICT and telent ensure the maintenance of vital '999' emergency response infrastructure, as well as continuing to expand the use of ICT technology so as to manage our resources more effectively in line with the risks facing firefighters, the communities of Merseyside and the organisational processes of the Authority.

ICT ILM, carried out by telent on behalf of the Authority, is done so in line with best practice from the ITIL framework. ITIL is a set of best practices and processes for the management of the ICT infrastructure and the delivery of ICT services and support.

The processes are mature and at the same time provide an infrastructure that is robust, secure, reliable and resilient; telent continues to deliver savings and innovation through supporting initiatives such as the Multi-Function Device (MFD) contract renewal, whilst continuing to provide a high-performing ICT service desk.

ICT and telent are responsible for ALM of commodity and Fire Control applications, whilst the Finance team and the Strategy and Performance Directorate are responsible for ALM for corporate and in-house developed applications.

1.2 Asset Management

ICT Asset Management is carried out by ICT on behalf of the Authority and it is done so in line with ITIL and Information Technology Asset Management (ITAM). The terminology 'ITAM' is interchangeable with ICT Asset Management.

In line with the organisation's policy for asset management, the lifecycle of an ICT asset has four distinct phases:

- Planning
- Acquisition
- Operation
- Disposal

And ICT follows five major principles:

- ICT asset management decisions are integrated with the strategic planning process
- ICT asset planning decisions are based on an evaluation of the alternatives, which consider the 'lifecycle' costs, benefits and risks of ownership
- Accountability is established for ICT asset condition, use and performance
- Effective disposal decisions are carried out in line with minimal environment impact
- An effective control structure is established for ICT asset management

Further information on how ICT manages ICT assets on behalf of the Authority can be found in the remainder of this plan.

Return to Top.

2 ICT Asset Management Strategy

ITIL ITAM is the set of business practices that join financial, contractual and inventory functions to support lifecycle management and strategic decision-making for the ICT environment. ICT assets include all elements of software and hardware that are found in the organisation's environment.

Under ITAM, ICT manages its assets effectively to help deliver its strategic priorities and services in line with risk, providing value-for-money-services for the benefit of the local community.

ICT has all of its ICT assets recorded in a Configuration Management System (CMS). This system is a database which records details of all the ICT assets and their age, thus enabling ICT to effectively manage the lifecycle of its infrastructure. The database where the asset information is held is on a Service Management System (SMS) called 'Remedy'. This gives the ability to link ICT incidents, assets and people, to enable a more in-depth trend analysis to be performed around ITAM decisions.

ICT has a service catalogue, which outlines all the ICT services provided. Included in this catalogue are references to the capacity planning, security and preventative maintenance carried out on ICT assets.

ICT has a robust reporting process to provide systematic and timely reporting of compliance and performance, enabling prompt asset-related decision-making regarding ICT assets.

ICT has a service pipeline. The service pipeline comprises new ICT services under development and these developments lead to new, or a change of use of, ICT assets (see Section 5 ICT Assets Service Pipeline for further details).

To manage the ICT five-year capital asset investment plan, ICT classifies spend into four categories:

- Underlying Spend
- ICT Project Spend
- Integrated Risk Management Plan (IRMP) Project Spend
- Fire and Rescue Service (FRS) National Project Spend

ICT has a five-year lifecycle-renewal policy for ICT hardware assets such as personal computers, devices and servers, at which point these ICT assets will be considered end-of-life (EOL).

ICT has a 5-10-year lifecycle-renewal policy for ICT hardware assets such as network switches and telephony, at which point these ICT assets will be considered EOL.

When an ICT asset is highlighted as EOL, its performance is assessed and, if required, a new asset will be purchased.

Adopting a best practice, asset management and configuration management solution allows ICT to understand:

- What ICT assets the Authority has
- Where they are located
- How well they are working
- How effectively they are supporting the business of the organisation

As a result, the following benefits have been realised:

- Accurate information on all ICT assets, providing ICT with the ability to deliver and support its services
- Trend analysis can be carried out against assets to aid incident and problem-solving
- Improved ICT security through advanced ICT asset control
- Improved financial planning through clear identification of all assets and their associated relationships
- Improved software licence management, ensuring legal compliance
- Increased confidence in ICT systems and ICT services
- Increased customer satisfaction

A snapshot-in-time list of the Authority's hardware ICT assets can be found in Appendix A – Summary of ICT Infrastructure Assets. This list can be requested and produced from Remedy to give a real-time view of the ICT asset holding. On a yearly basis, the list is produced for insurance calculation purposes.

The system is also used for various analytical tasks including:

- Identification of obsolete ICT assets based on a purchase date
- Identification of current and previous ICT asset owners
- ICT asset rationalisation
- Role Based Resourcing (RBR)

All ICT assets pass through a configuration management process where they are allocated and labelled with a unique asset reference number.

In line with ITIL, ICT has a Definitive Media Library (DML) to improve the way it tracks software and performs ALM.

Return to Top.

3 ICT Infrastructure Asset Monitoring Activities

ICT maintains an up-to-date service catalogue which outlines all the ICT services provided. Included in this catalogue are references to capacity planning, security and preventative maintenance, all of which are examples of activities carried out on ICT assets.

3.1 Capacity Planning

'Capacity planning is used to ensure that the Authority has adequate capacity to meet its demands, even during periods of extreme high usage and growth. This includes but is not exclusive to: estimation of disk space, computer hardware, software, and network infrastructure that will be required over a set amount of time.'

Capacity is calculated in various ways depending on the system and specific requirements from ICT.

Regular storage reports are run on servers and file shares, which are used for current and projected growth estimations using bespoke software.

Additionally, network management software is utilised to manage the capacity of all network links used within the Authority's Wide Area Network (WAN) and Local Area Network (LAN).

3.2 Security

'The Authority requires multiple levels of security on managed devices to defend against malicious behaviour and mitigate the risk to the Authority.'

Patching is one of the most important parts of a cyber-security strategy; keeping things on the latest version, in most cases, means greater security.

Merseyside Fire and Rescue Authority (MFRA) has a patching policy in place and it applies to each area of the ICT infrastructure. Patching is conducted based on the assessment of risk. This policy is prudent, balancing the need to reduce the amount of downtime to critical systems with cyber-security risk.

To assist in the automation of processes and administration of the status of both end point devices and servers, an ICT infrastructure discovery tool – Nexthink – has been deployed to enable the ICT estate to be tightly managed and, importantly, easily reported on.

This provides security by design, audit and assurance; Nexthink highlights hardware and software, if it is not fully patched and up-to-date, to allow MFRA to adhere to the required patching level defined by the Emergency Services Network (ESN) Code of Connection (CoCo).

A key response to cyber-security is Security Information and Event Management (SIEM) and MFRA is implementing LogPoint as a SIEM tool. This ensures that the appropriate levels of security information are both readily available and stored for an agreed length of time.

Forcepoint is used to protect end-user devices from spam, viruses and other malicious threats via e-mail and internet. The solution configuration is hybrid hosted and on-premise. Sophos Endpoint Protection is used to secure the Authority's systems – including, but not limited to, Windows servers, Windows desktops, Windows laptops, iPads and mobile devices – against viruses, malware, advanced threats and targeted attacks.

With the rollout of the Samsung mobiles phones we will be able to take advantage of using Mobile Device Management (MDM) for all corporate devices (company-owned devices), protecting our information more securely than in the past.

MDM is provided by Sophos Mobile Control and provides a full suite of management and security tools for any device, covering the important capabilities of management, security, productivity and compliance.

With the introduction of General Data Protection Regulation (GDPR) and ESN, in addition to the ever-changing security threats from mobile malware and data loss, blue light organisations and partner agencies have realised that they require effective MDM to complement existing security protocols.

Devices containing potential sensitive data are encrypted up to 256 bits using Advanced Encryption Standard (AES).

3.3 Device Preventative Maintenance

'telent is responsible for device preventive maintenance, including planned maintenance activity designed to improve equipment life and avoid any unplanned maintenance activity.'

The Authority requires desktops and laptops to be configured with Sophos Anti-Virus and Windows Updates via a Windows Server Update Services (WSUS) Server.

Recently, System Centre Configuration Manager (SCCM) has been introduced. SCCM is a systems management software product developed by Microsoft for maintaining large groups of computers running Windows 10. SCCM will be initially used to provision the Toughpads which were procured in 2017/2018.

Sophos performs a full daily scan on each device and alerts via desktop and e-mail alerting if any issues are reported.

Windows critical updates are installed via the WSUS server and recommended updates are reviewed and tested before installing on end-user devices.

BIOS/firmware patching is performed when a device is re-imaged from the software library or if a specific fault occurs'.

N.B. The full ICT service catalogue is too large to be an attachment but it can be accessed on request to ICT.

Return to Top.

4 ICT Infrastructure Asset Monitoring Reports

Effective ICT asset management requires a monitoring process to provide systematic and timely reporting of compliance and performance, to enable prompt asset-related decision-making. ICT prepares and publishes the following reports to fulfil this function:

4.1 Service Desk Performance Report – Monthly

The monthly ICT Service Desk Performance Report is provided to enable telent, ICT and the Authority's officers to review the service delivery of ICT for the Authority and, if required, any escalation can be taken to the Strategy and Performance (S&P) ICT and Information Management (IM) Board.

4.2 ICT Infrastructure Usage Report – Monthly

The monthly ICT Infrastructure Usage Report is provided to enable telent, ICT and the Authority's officers to review and discuss infrastructure usage, review the top 10 users of each asset and share the information with the Authority's budget holders.

4.3 Information Security Report – Quarterly

The monthly Information Security Report provides telent, ICT and the Authority's officers (including the Senior Information Risk Owner [SIRO]) with relevant information that supports the Authority's information security policy. It is posted on the portal and is reviewed at the Protective Security Group (PSG) Meeting.

4.4 Problem Management Reports – Monthly

In line with ITIL service management processes, this report provides the statistical analysis and evidence that supports problem management.

Problem management seeks to proactively minimise incidents by identifying and recording problems and known errors within the ICT infrastructure. Errors within ICT infrastructure can cause repeated incidents, which have an adverse effect on the business. Identifying and removing errors can reduce the number of incidents over time.

4.5 Major Incident Management Reports – Ad Hoc

Whenever a major ICT Incident takes place, a Major Incident Management Report is produced and reviewed with a view to establishing lessons learnt and to feed back into the ICT service catalogue.

Return to Top.

5 ICT Assets Service Pipeline

The service pipeline comprises new ICT services under development and these developments lead to new, or a change of use of, ICT assets. ICT has seven main areas associated with the service pipeline:

- ICT Service Requests
- ICT Business Relationship Management
- ICT Continuous Service Improvement (CSI)
- Lifecycle Management
- ICT Strategic Framework
- ICT & IM S&P ICT Board
- Other ITIL Standards

A full list of key ICT projects can be found in Appendix B – Key ICT Projects and Activities.

5.1 ICT Service Requests

The ICT Service Desk issues ICT request forms to allow users to request simple technical changes, information, enquiries or hardware and software changes, e.g. mobile phones.

For certain ICT requests, an approval route through the ICT Infrastructure Manager is needed. The ICT request process is fully integrated in the CMS, with all changes being documented.

5.2 Business Relationship Management

Reporting to the Head of Technology; the Business Relationship Manager (BRM) acts as the liaison between ICT and the organisation to understand its strategic and operational needs. The BRM acts as a single point of contact for senior stakeholders, ensuring understanding of available and future ICT infrastructure services and promoting financial and commercial awareness in order to deliver value for money. The BRM represents the organisation's needs and interests within ICT, contributes to the ICT CSI process (see below) and assists with the supervision and prioritisation of ICT infrastructure services projects.

5.3 ICT Continuous Service Improvement (CSI)

The purpose of the ICT CSI meeting is to ensure that cost-justifiable ICT capacity in all areas of ICT exists and is matched to the current and future agreed needs of the business in a timely manner. A key focus is on increasing the efficiency, maximising the effectiveness and optimising the cost of services and the underlying ICT service management. Meetings follow a six-week cycle and the process is documented in the CSI register. This CSI process is now firmly embedded in the ICT department, and the key benefits have been:

- Clarity of ownership
- Clarity of requirements

- Clarity and management of costs
- Visibility and tracking progress
- Forward planning
- Resource scheduling
- Identifying duplicate effort across the Authority's departments and/or stations
- The ability to utilise information from archive

5.4 Lifecycle Management

The ICT challenge is to provide the most functional, flexible ICT infrastructure possible, to host the applications that deliver benefits to the organisation, all at the lowest cost of ownership. Meeting that challenge systematically through having the right people in the right structure, ILM, ALM and best practices such as ITIL can lead to improvements in efficiency, performance and cost management.

5.4.1 ICT ILM

ILM encompasses the planning, design, acquisition, implementation and management of all the elements comprising the ICT infrastructure.

5.4.2 ICT ALM

ALM encompasses the planning, design, acquisition, implementation and management of all the elements comprising Fire Control and commodity application portfolios.

5.4.3 ITIL

ITIL is a globally accepted approach and set of practices for IT Service Management (ITSM) that focuses on aligning ICT services with the needs of the business.

5.5 ICT Strategic Framework

The ICT Strategic Framework is a cycle of four meetings that takes place on an annual basis and the output feeds into the S&P, ICT & IM Board.

The ICT Strategic Framework is part of the governance applied to the delivery of the telent ICT managed service; meetings are held once a quarter to cover one of three topics. There are two 'Innovation and Technology Forums', an 'Efficiency and Value for Money Meeting' and a 'Strategy and Alignment Meeting' held each year.

The ICT Strategic Framework ensures that the ICT managed services contract:

- Is working effectively
- Has its strategic goals set and aligned with the needs of the Authority
- Improves efficiency of arrangements and delivers mutually beneficial savings and efficiencies

5.6 Strategy and Performance (S&P) ICT & IM Board

There are three monthly thematic S&P boards in place: ICT & IM (with Finance and System Support); Equality and Diversity (E&D) and Performance Planning and Risk Information; which means a thematic S&P ICT & IM Board will meet every three months. The purpose of the S&P ICT & IM Board is to ensure that ICT, application provision and information management are coordinated and aligned to ensure the mission and objectives of the Authority are delivered as effectively as possible.

5.7 Other ITIL Standards

- A Change Advisory Board (CAB) has been set up which will ensure that only authorised changes are deployed to the Authority's infrastructure. This will also improve the communication between key system owners and ICT

- ICT maintains and develops a DML. It ensures that:

    - A secure compound is established in which master copies of all authorised versions of the organisation's software are stored and protected

    - All documents pertaining to applications are stored in a central location, e.g. number of users, location of users, contact details of suppliers and Service Level Agreements (SLAs)

- ICT sets minimum release management standards which third party suppliers are expected and contracted to reach

Return to Top.

6 ICT Asset Replacement Policy

ICT has in place procedures to trace the acquisition, deployment, management and disposal of ICT assets under its control.

Some of the primary goals for asset replacement are:

- To develop an appropriate type of replacement mix based on each asset and its behaviour
- To ensure value for money
- To meet desired/acceptable level of risk
- To enable realistic forecasts of future events

6.1 ICT Asset Purchasing

In the main, the Authority owns the ICT assets. When ICT assets are purchased by ICT, the following applies:

- For small quantities of ICT commodity items; the Authority's ICT outsourced partner will seek quotes and the Authority will purchase

- For large quantities of ICT commodity items; the Authority's ICT outsourced partner will specify requirements but the Authority's procurement team will run mini-competitions and the Authority will purchase

- For ICT assets which require complex installation or if priority support is required; the Authority's outsourced partner specifies and purchases the item on the Authority's behalf and then the Authority pays via change control

- In such cases the Authority's ICT outsourced partner is requested to run a mini-competition and produce options for the Authority to select

- Purchase is done via the contract change control procedure, and the Change Control Note (CCN) is signed off by ICT, Procurement and Legal. No mark-up is charged by the Authority's ICT outsourced partner, as the contract makes provision for commercial services

6.2 ICT Asset Disposal

ICT has in place procedures for the disposal of ICT assets via a company called 'Computer Waste'. Computer Waste is an Authorised Treatment Facility (ATF), fully registered by the Environment Agency (EA). The company specialises in the recycling of waste electrical and electronic equipment (see WEEE).

- All ICT assets disposed of with Computer Waste are recorded on a waste transfer note that is signed and presented to the Authority for audit purposes

- Hard drives are destroyed on the Authority premises, witnessed by an employee of telent, and an accompanying destruction certificate is presented to the Authority for audit purposes

6.3 ICT Hardware Assets

ICT has a five-year lifecycle-renewal policy for ICT hardware assets such as PCs, tablets, mobile devices and servers, at which point ICT Assets will be considered end-of-life. A three-year equipment life was considered but the increased capital spend was deemed to be excessive.

Furthermore, the proliferation of devices along the wide spectrum of ICT presents opportunities and challenges to ICT, as well as budget challenges to the organisation. There is a policy of using shared MFDs and having one MFD per function to replace printers. This printer rationalisation has contributed to budget savings.

RBR is undertaken by ICT, evaluating the agile provision of ICT equipment at stations, SHQ, TDA, Vesty One and 'incidents', based on the roles of the staff housed or present there.

An ICT Asset Based Resourcing (ABR) initiative is also in place as a check and balance to RBR, ensuring operational vehicle assets match the role of firefighters and senior officers who use such vehicles.

ICT has a 5-10-year lifecycle-renewal policy for ICT hardware assets such as network switches and telephony, at which point ICT assets will be considered end-of-life.

ICT assets could also be replaced on an ad-hoc basis but this would lead to difficult budget forecasting, with some years seeing larger budget increases than others. If, however, ITIL problem management analysis identifies an ICT hardware asset that is repeatedly problematic, causing a break in service, the equipment would be considered for replacement before its five-year equipment life had expired.

6.4 ICT Asset Movements 2019/2020

The key ICT asset movements to highlight in 2019/2020 are:

- To date 120 Surface Pros have been rolled out and RBR is being viewed as Business as Usual (BAU)

- The deployment of Firecoders from Multitone Electronics replacing station turnout PCs

- The replacement of 200+ Windows Smart Phones with the Samsung Xcover 4 or the Samsung J6s. In the financial year the Samsung J6 has been superseded and trails of potential replacements phones are underway

- The commissioning of the Vesty Road Resilient External Wireless WAN solution based on Siklu point-to-point radio communications

- The successful go-live of new Mitel Phone solution and a move to SIP (Digital) Trunking for Administration Telephony

- The replacement of the Storage Area Network (SAN) with a new HP Modular Smart Array Solution

Return to Top.

7 Fire Control Applications and Hardware Assets

Reporting to the Head of Technology, the ICT Application and Infrastructure Manager (Fire Control) works with the Authority's outsourced ICT partner to carry out appropriate lifecycle management to ensure successful ICT service delivery in line with SLAs. Activities include:

- Following of best practice ICT asset management
- Application or infrastructure replacement or refresh
- Spare holding to replace faulty equipment which is one method in ensuring SLAs are met
- Year-on-year preventative maintenance in mid-October prior to the bonfire period. This is done for both Primary and Secondary Fire Control infrastructure and applications
- Regular relocation exercises to Secondary Fire Control

7.1 Six High Level Areas of ICT in Fire Control.

- CAD; this is where incoming emergency calls are logged and the appropriate resources mobilised to incidents. The Authority uses the Vision 3 FX CAD application
- Management Information System (MIS); providing senior officers with real-time incident information, and the organisation with incident history for trend analysis & business intelligence. The Authority uses the Vision 3 FX BOSS application
- An Integrated Communications Control System (ICCS); an ICCS is found at the centre of modern day control rooms. All communications that go into the control room such as 999 telephony calls, administration telephony calls, radio communication and CCTV are routed via the ICCS. The control room staff can then manage these various communication channels from one place on their desktop by accessing the ICCS.
- Wide Area Radio Scheme; emergency services rely on seamless radio communications coverage to effectively perform their daily tasks. The Authority, in line with the police and ambulance, uses Airwave. The national project Emergency Services Mobile Communications Programme (ESMCP), when completed, will replace Airwave with the ESN.

- Data Mobilisation; Fire Control can mobilise crews to incidents by sending a message to the Mobile Data Terminal (MDT) installed in the appliance. The Authority uses the SEED application

- The Station-end turnout solution installed in every community fire station is comprised of a number of various hardware and software components and subsystems the key one being a Firecoder from Multitone Electronics. The solution involves automatically unlocking doors; switching on of lights; sounding the alarm and printing the emergency turnout information on the fire station printer. This enables crews to respond to emergency turnouts in a safe and efficient manner.

7.2 CAD-MIS Upgrade

In September 2017, the Authority approved a project to replace Vision 3 FX CAD & Vision 3 MIS applications supplied by Capita.

In July 2019 Members approved the upgrade of Vision 3 FX to Vision 5 along with a refresh of the associated components of the Fire Control infrastructure at an expected cost of £820k. This is phase one of a two-phase project to deliver risk critical enhancements with an estimated budget of £950k.

Contracts with Capita have been signed to deliver an upgrade from Vision 3 to Vision 5. A project launch meeting is scheduled for the 3rd week in January 2020 followed by a project board meeting the week after. The hardware orders are being progressed and delivery is expected in February 2020. The Capita Project Manager (PM) is in place and an interim telent PM is also in place whilst recruitment continues.

By mid-2020 to end-2020, with the upgrade to Vision 5 complete, the position will be to take stock and determine what the Authority's next generation Fire Control solution will be and whether it will be shared with other emergency services.

Budgetary costs will be fed into the five-year capital budgeting process once the next generation solution is determined.

7.3 Emergency Service Network (ESN)

The national transition period for ESN is currently 2021-2025 with the North-West region expected to begin transition Q2 2021.

In 2017/2018 a new capital scheme (IT058) was raised to cover future ESN costs. This is additional to the capital schemes that have been set up to facilitate the Home Office funded preparation works. Capital schemes remain largely unaffected; however ESN device refresh and phased integration costs could increase and should not be ruled out.

Future revenue costs for ESN remain unclear. Home Office costs associated with the ESN are expected to be 50% of the current Airwave bill, however, it remains unclear how this will influence future grants.

Work is ongoing with the Home Office to undertake early-adopter trials of ESN products. This aims to reduce the overall project transition period and associated costs. MFRA are also testing early ESN products (Direct 2.0+) which could deliver system enhancements ahead of transition and potentially lower future integration costs.

Return to Top.

8 ICT Commodity Application Software

ICT is responsible for ensuring the Authority has an ALM strategy for all its commodity applications. ICT works closely with all departments to develop and manage organisational commodity applications and agree and monitor ICT application SLAs.

8.1 Microsoft Software: Enterprise Agreement (EA)

The Authority's strategic direction is to use Microsoft products.

In 2018, Microsoft, in collaboration with the Crown Commercial Service (CCS), released details of the next generation framework of public sector pricing. The Digital Transformation Arrangement (DTA) came into effect from 1st May 2018, to run for three years to 30th April 2021. The DTA provides greater access and discounts to assist customers in their use of Microsoft cloud technologies.

To continue to use the latest versions of Microsoft products, such as Window Server, Windows 10 and Office, during 2019/2020 MFRA will need to renew its Microsoft EA for a further three years from April 2020.

In renewing MFRA's Microsoft EA, MFRA will need to sign up to the Microsoft DTA.

The cost of the existing EA, under the now-defunct Microsoft EA Cloud Transformation Arrangement (CTA), is £206k p.a. The initial guide pricing based on 'as is' under the new Microsoft EA DTA is £261k.

This means a potential capital budget increase of £55k p.a. for three years from 1st April 2020.

8.2 Anti-Virus and E-mail Filtering

The ICT-selected anti-virus software, Sophos, protects the Authority from computer viruses and any other threats which may try to enter the Authority's network.

The ICT-selected e-mail filtering system, Forcepoint, is used to filter e-mail and quarantine non-legitimate e-mails via the process of word detection. The words that result in the email being quarantined are recorded in a database and analysed on a monthly basis.

The licences for the anti-virus and e-mail filtering products are procured on a 3-5-year lifecycle and prior to any future renewal, a fit-for-purpose exercise will be carried out.

Return to Top.

9. Corporate and Financial Application Software

9.1 Application Classification

Applications are managed through their lifecycle in collaboration with application owners, and are given a classification to identify their status. The classifications include:

New	Conceived, in planning phase, under construction or newly deployed
Emerging	In production or licenses have been purchased, but in limited use, such as a pilot
Mainstream	In production and actively being used
Containment	In production for a specific or limited purpose
Sunset	In production with scheduled retirement in progress
Prohibited	No longer used

See Appendix D – Application Status for a full list of applications.

9.2 Application Requests

Any Department with a requirement for a new or replacement application must, in the first instance complete the Application Request Form. The form can be accessed from the S&P homepage on the Portal. The form captures the following information:

- Identified application sponsor and owner
- Organisational need/value
- Risks to the organisation
- Legislative requirements
- Potential efficiency savings
- Collaboration considerations
- Budget allocated for this application

If the application request is approved for progression to the next stage, a further business case is required, detailing the market engagement carried out, cost benefit analysis, and recommendations.

9.3 Application Gateway Team

The purpose of the Application Gateway Team is to provide the Authority with effective governance arrangements for new or replacement applications. The Application Gateway Team are responsible for approving and prioritising the advancement of new or replacement applications within the organisation. See Appendix D – Application Status for a full list of applications.

9.4 Application Development

9.4.1 Application Toolkit

The Application Development Team utilises a suite of products which assists with the development of internal applications.

Azure DevOps	Azure DevOps is a Microsoft product that provides version control, reporting, requirements management, project management, automated builds, lab management, testing and release management capabilities. It covers the entire application lifecycle, and enables DevOps capabilities.
Azure IaaS	Infrastructure as a service (IaaS) provides a secure and scalable infrastructure.
Azure SaaS	Software as a service (SaaS) allows users to connect to and use cloud-based apps over the Internet.
Visual Studio	Microsoft Visual Studio is an integrated development environment. It is used to develop computer programs, as well as websites, web apps, web services and mobile apps.
ReSharper	ReSharper is a popular developer productivity extension for Microsoft Visual Studio. It automates coding routines by finding compiler errors, runtime errors, redundancies, etc.

9.4.2 DevOps

DevOps is the union of people, processes and products to enable continuous delivery of value to our end users. The combination of 'Dev' and 'Ops' refers to replacing siloed 'Development' and 'Operations' with multidisciplinary teams that work together with shared and efficient practices and tools. DevOps has been adopted as a recognised framework to ensure the success of any app development and to align developed apps and infrastructure; Dev being the Application Development Team, Ops being ICT/telent.

9.4.3 Development Portfolio

The application development portfolio currently consists of the following applications.

Application	Classification
OPS (Operational Performance System)	Mainstream
SOFSA (Simple Operational Fire Safety Assessment)	Mainstream
National Resilience Application	Emerging
SIRAH (Site Information Risk And Hazard)	Emerging
The Hub	New
Protection	New
Prevention	New

Return to Top.

10 ICT Asset Capital Spend Strategy

10.1 ICT Asset Investment Process

To manage the ICT asset investment process, ICT classifies spend into four categories:

- Underlying Spend
- ICT Project Spend
- IRMP Project Spend
- National FRS Project Spend

These are explained in the following table:

	Spend	Why	Benefit
Underlying Spend	Spend on the existing ICT infrastructure including software, devices, servers, networks and voice communication e.g. upgrade of station switches	This spend stops the ICT infrastructure and any software becoming out of date	More than just 'keeping the lights on' An ICT-enabled organisation whose systems are robust, secure and resilient, with the ability to accommodate change
ICT Project Spend	Projects that: Deliver Authority changes, deliver step changes in technology e.g. MDT evolution	This spend delivers value for money, innovation and savings where appropriate	ICT accommodating change with a focus on a sound business case and clear deliverables
IRMP Project Spend	Spend on specific IRMP projects where ICT is a major enabler e.g. station change	This spend delivers the Authority's IRMP	Safer, stronger communities; safe effective firefighters. Releasing budget for frontline resources
National FRS Project Spend	Spend on specific national projects where ICT is a major enabler e.g. ESMCP	Spend to align the Authority's systems to national initiatives	Protecting public safety and increasing national resilience

The 2020/2025 Five-Year Capital Plan can be found in Appendix C – 2020/2025 ICT Five Year Capital Plan

10.2 Review of the Current Capital Programme

ICT carries out an annual full review of its capital budget. The basis for the review is to:

- Determine if any reductions in planned spend was possible, and/or
- Determine if the asset life could be reviewed (extended) to reduce the frequency of replacing assets etc., and/or
- Determine if anything else could be done to reduce the level of planned borrowing and therefore reduce the impact of debt servicing costs on the future revenue budget

This asset management plan has been updated to reflect this review.

10.3 The Emergence of Cloud Computing.

The ICT cloud strategy is:

'Application development in the public cloud to transform existing processes to meet business needs, whilst exploring the public cloud, hybrid cloud and on-premise, to deliver dynamically automated ICT infrastructure management, the promise of reduced costs and the ability to run mission critical applications.'

The move to the cloud and taking ICT as a service, rather than buying a product and installing it on ICT equipment, moves the cost of ICT from being mostly a capital, one-off cost to an on-going revenue cost. Therefore, investment in ICT over the coming years will not be a case of deciding where to spend the capital budget, but instead one of choosing between spending revenue on ICT systems or on other priorities.

ICT will work closely with Finance to achieve this potential transition over the coming years.

Return to Top.

11 Glossary

ABR	Asset Based Resourcing
AES	Advanced Encryption Standard
ALM	Application Lifecycle Management
ATF	Authorised Treatment Facility
AV	Audio visual
BAU	Business as Usual
BIOS	Basic Input/Output System
BRM	Business Relationship Management or Manager
CAB	Change Advisory Board
CAD	Computer Aided Dispatch
CCN	Change Control Note
CCS	Crown Commercial Service
CMS	Configuration Management System
CoCo	Code of Connection
CSI	Continuous Service Improvement
CTA	Cloud Transformation Agreement
DML	Definitive Media Library (previously Definitive Software Library, DSL)
DTA	Digital Transformation Arrangement
E&D	Equality and Diversity
EA	Enterprise Agreement *or* Environment Agency
EOL	End-of-life
ESMCP	Emergency Services Mobile Communications Programme
ESN	Emergency Services Network
FDS	Functional Design Specification
FRS	Fire and Rescue Service
GDPR	General Data Protection Regulation
IAAS	Infrastructure as a Service
ICCS	Integrated Communications Control System
ICT	Information and Communication Technology
ILM	Infrastructure Lifecycle Management
IM	Information Management
IRMP	Integrated Risk Management Plan
ITAM	IT (or ICT) Asset Management
ITIL	Information Technology Infrastructure Library
ITSM	IT Service Management
LAN	Local Area Network
MDM	Mobile Device Management
MDT	Mobile Data Terminal
MFD	Multi-Function Device
MFRA	Merseyside Fire and Rescue Authority
MIS	Management Information System

OPS	Operational Performance System *or* short form for Operations
PC	Personal Computer
PIPS	Planning Intelligence and Performance System
PM	Project Manager
PSG	Protective Security Group
RBR	Role Based Resourcing
S&P	Strategy and Performance
SAAS	Software as a Service
SAN	Storage Area Network
SCCM	System Centre Configuration Manager
SIEM	Security Information and Event Management
SIRAH	Site Information Risk and Hazard
SIRO	Senior Information Risk Owner
SLA	Service Level Agreement
SMS	Service Management System
SOFSA	Simple Operational Fire Safety Assessment
SQL	Structured Query Language
StARS	Staff Attendance Recording System
TDA	Training and Development Academy
WAN	Wide Area Network
WEEE	Waste Electrical and Electronic Equipment
WSUS	Windows Server Update Service

Return to Top.

Appendix A – Summary of ICT Infrastructure Assets

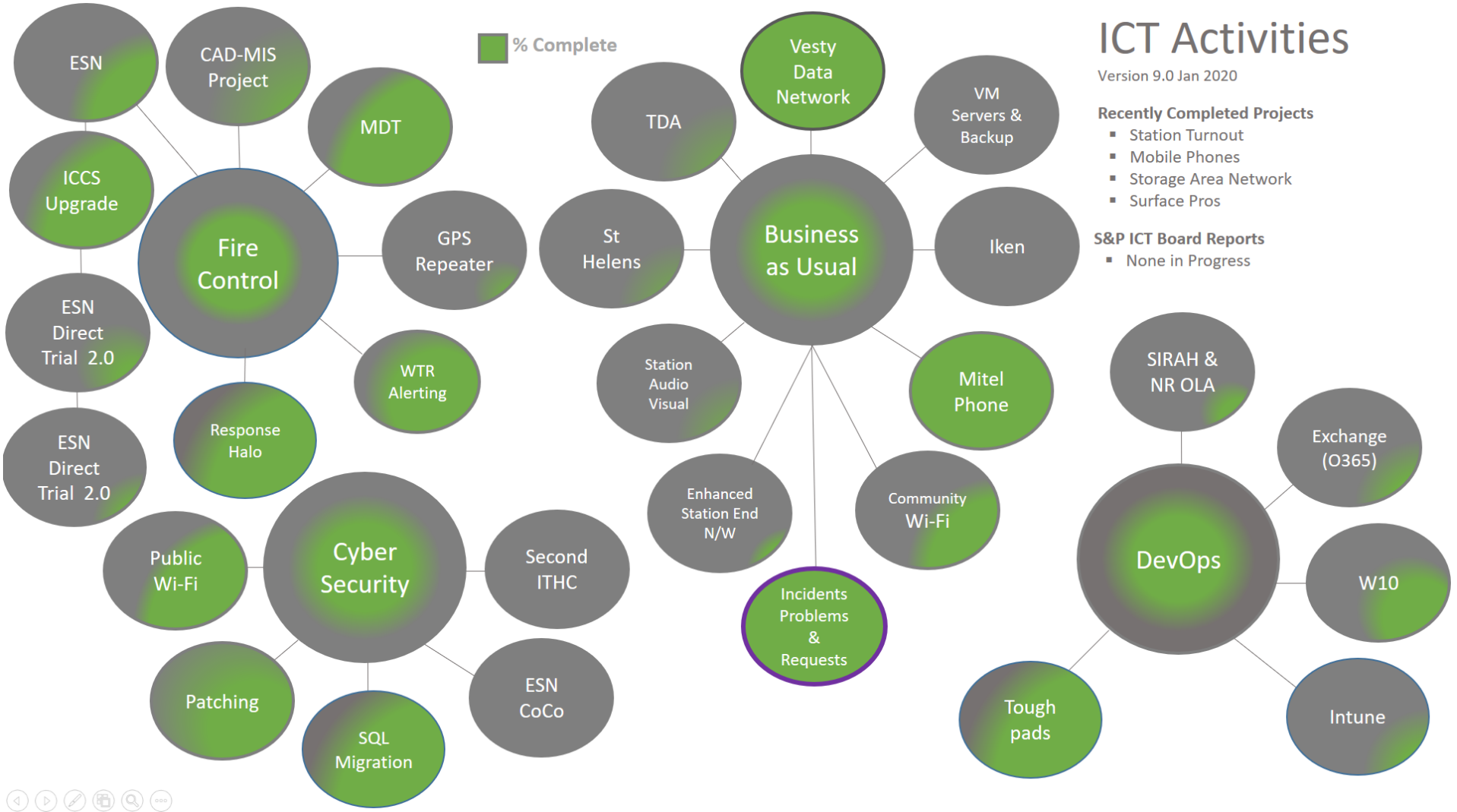
Fire Control Services and Infrastructure	Quantity
Physical Servers (Licensed as part of C&C Solution)	19
Virtual Servers (Licensed as part of C&C Solution)	1
C&C Desktops (Licensed as part of C&C Solution)	27
C&C Monitors	29
DS3000 ICCS Server	1
DS3000 ICCS Client	20
DS3000 ICCS touchscreen	20
Capita VAIU	20
Airwave San H radio gateway	1
Stateboard	3
Alerter Masts	8
Alerter Devices (multitone)	178
UHF Radio Set 2 (GP340)	149
UHF Radio Set 3 (GP340 Atex) for breathing apparatus	42
UHF Radio Set 4 (F61)	11
UHF Radio Set 5 (M1 Euro)	18
Station End Firecoders	27
Station End Turnout Printers	36
Station End Auxiliary Relay Unit (ARU)	32
Station End Amplifiers	35
Station End UPS	40
IMT/IGMS Vehicles	2
Packets Atex/Marine Band/Motorola	266
Fire Control Headsets	40
Mobile Data terminals	79
Mobile Data Terminal touchscreen	96
Appliance printers	85
Airwave mobile radio SAN A	115
Airwave SAN J Radio	65
Airwave SAN B Radio	11
MDT Pump Bay Voice Terminal	85

Administration Infrastructure, Managed Servers & Desktop	Quantity
Physical Servers	65
Virtual Servers	124
Desktops *(A limited number of users have two monitors*)	631
Laptops *(Most People have an external monitor)*	324
Docking Stations *(Most Laptop Users have an external monitor)*	309
Tough Books	60
Monitors	903
Non-Standard Printers (*not Konica devices*)	9
Konica Minolta Multi-Function Devices (Contracted to August 2022)	53
Konica Minolta Desktop Print Devices (Contracted to August 2022)	13
ASA 5515X - Security Appliance	5
ASA 5510 - Security Appliance	3
ASA 5506X - Security Appliance	3
FPR1010 - Security Appliance	2
Router c819	2
Router c2921	2
Router c1841	23
Router c1921	7
Switch c4510r-e	1
Switch c4507r+e	1
Switch c3850	2
Switch c3750	30
Switch c3560	5
Switch c3550	40
Switch c2960	22
Wireless Controller	1
Wireless Access Points	98
Mitel IP Sets	650
Mitel 5310 Conferencing Phones	10
HP Tape Library 8096	1
HPE MSA 2050 (File SAN)	2
HP MSA 2312i (Portal SAN)	1
Panasonic Toughpads	58
Microsoft Surface Pros	122
Microsoft Surface Books	10
Microsoft Surface Laptop	12
Microsoft Surface Go	13
Ubiquiti Nanobeam 5AC Gen 2	2
SIKLU Radio Link	6

Miscellaneous	Quantity
Mobile Phones	434
iPhones	10
Smartphones	216
MTPAS Enabled Mobile SIMS	96
MDT Enables Data SIMS	87
iPad	54
USB Encrypted USB devices	137
3G/4G Dongles	34
Modem	51
Battery Chargers	142
Smart Boards	31
Epson Wall Mounted Projector	5
Barco Click Share	5
Samsung Screens	16
IPTV - Server	1
IPTV - Gateways	3
IPTV - Receivers	31
Remote Access Tokens (Celestix)	100
Running Call Phones	31

Return to Top.

Appendix B – Key ICT Projects and Activities



Fire Control

Item	Description	Status
ESN	ESN will replace the communication service delivered by Airwave with a national mobile voice and data service for all three emergency services.	A programme of works is ongoing including Airwave enhancements and local ESN trials to ensure 'Prime' (the final ESN product) is delivered in 2021.
ESN Direct 2.0 Trial	MFRA has agreed to undertake ESN Product Direct 2.0 trials; testing the delivery and use of handsets on behalf of the Home Office.	The preparation and planning phase of the Direct2.0 trials for handsets began in August 2019 and test scheduling is underway with the intention of starting a formal 6-week testing phase in Feb/March of 2020.
ESN Early Adopter	MFRA is being considred as a lead for the Fire Sector in the development and delivery of small to large scale operational exercises, in order to test the final 'Prime' ESN product in 2021.	Discussions, which started in December 2019, are ongoing with the Home Office to develop MFRA as an 'Early Adopter' of ESN and trial devices.
ICCS Upgrade	This project has four programmes of works which are required to connect the Capita DS3000 ICCS to the new Emergency Services Network (ESN).	The ESN DSNP link is installed and a Phase 1 technology refresh of the ICCS was completed in March 2018. Following a successful Direct 2.0 formal 6-week testing phase, it is likely that a period of enhanced integration of the ESN to our ICCS and CAD will follow.
CAD-MIS Project	Replacement of computer hardware and the upgrading of Vision CAD and Vision BOSS applications to deliver an enhanced CAD for 2020.	Now in contract with Capita to deliver an upgrade from Vision 3 to Vision 5. A project launch meeting is scheduled for the 3rd week in January 2020, followed by a project board meeting the week after. The hardware orders are being progressed and delivery is expected in February 2020.
MDT	Rollout to frontline appliances of the new Mobile Data Terminals (MDTs) with the Airbus mobilisation and risk app.	Work to populate Airbus with risk information and operational documents continues, and rollout of the MDTs (CF33s) is due for completion in May 2020.
Station Turnout	Rollout of Multitone equipment to replace existing station end turnout PCs.	Complete.

Business as Usual (BAU)

Item	Description	Status
Vesty Data Network	To provide a cost-effective wireless solution to connect the MFRA Vesty Road buildings to MFRA SHQ network infrastructure.	Completed. The commissioning of the Vesty Road Resilient External Wireless Wide Area Network solution based on Siklu point-to-point radio communications.
Mobile Phones	Rollout of Samsung Xcover 4 and J6 mobile phones to replace the existing Windows mobile phones.	Complete. The replacement of 250+ Windows smartphones with the Samsung Xcover 4 or the Samsung J6s.
Mitel Phone Upgrade	Replacement of the legacy Mitel IP telephony solution to replace existing hardware due to it becoming end of life.	November 2019 saw the successful go-live of new Mitel phone solution and a move to SIP (digital) trunking for administration telephony.
Incidents and Problems	These are the day-to-day disruptions to the ICT Service outside of BAU ICT Services. e.g. loss of internet, e-mail.	At the time of writing there are no major incidents that are outstanding.
TDA	The project comprises the refurbishment of the TDA and the refurbishment of Station 19. TDA is home to Secondary Fire Control and Disaster Recovery.	ICT tracker is in place to capture scope of the ICT requirements.
Enhanced Station End Network	In line with the Asset Management Plan and increased data demands, the network links to stations will be increased to 100mb from 10mb.	Commercial discussions are ongoing with the supplier – Virgin Media and are expected to be completed in January 2020. Once agreed, a phased upgrade plan will then be implemented to minimise disruption. Note: The existing Virgin Media contract expires 30th June 2020.
Station Audio Visual	The replacement of existing projectors and smartboards with new projectors and screens or 'Clevertouch' TVs, at non-PFI stations only.	Projector numbers, model and approximate costs have been confirmed. Waiting on more accurate quotes from PureAV for two stations. Waiting on Clevertouch demonstration at Mather Avenue Police Training School. Ops Response has expressed an interest in seeing the demonstration.

Other Highlights

Item	Description	Status
Surface Pros	Rollout of Surface Pros in line with Role Based Resourcing (RBR).	To date 120 Surface Pros have been rolled out and Role Based Resourcing (RBR) is viewed as Business as Usual.
Exchange Upgrade (O365)	Exchange migration to Microsoft-hosted O365 mailboxes and user adoption of O365 collaboration functionality.	telent is using Microsoft Deployment Planning Services (DPS) days and the Microsoft FastTrack service to plan and prepare for the upgrade.
Windows 10 (W10)	Over and above the Toughpads and Surface Pros, this is the full rollout of W10 across the organisation.	Video guides have been completed and are on the portal. The service desk is currently converting W7 user guides to W10 before the phased rollout begins.
Intune	Implementation of Intune as the primary Mobile Device Management (MDM) platform (replacement for Sophos Mobile Control).	Intune has been installed, configured and is currently being tested with the new Toughpad build, along with the latest Android mobile Operating System (OS).
Toughpads	Rollout of Toughpads for the SIRAH app.	Toughpads are ready to roll out in line with the SIRAH rollout.
IT Health Check (ITHC) Roadmap	ITHC remedial security activities to ensure readiness for transition onto the ESN.	With most remedial actions complete, it only remains to carry out a second ITHC and complete the ESN Code of Connection (CoCo).

Return to Top.

Appendix C 2020/21 – 2023/2025 ICT Five Year Capital Plan – Draft

ICT - Proposed Budget 2019/20 to 2024/25

Type of Capital Expenditure	Total Cost £	2019/20 £	2020/21 £	2021/22 £	2022/23 £	2023/24 £	2024/25 £
IT002 ICT Software							
Software Licences	**12,000**	2,000	2,000	2,000	2,000	2,000	2,000
New Virtualistation Infrastructure	**146,000**	71,000				75,000	
3 Year Licences Antivirus & Filtering							
5 Year Antivirus & Filtering Software	**200,000**				200,000		
MDT Software Solution Refresh	**100,000**				100,000		
Microsoft SQL Upgrade	**50,000**					50,000	
Logpoint Security Information and Event Mgmt (SIEM) Refresh	**160,000**		80,000			80,000	
Windows 7 Security Assurance (Extended Security Update)	**12,000**		12,000				
Microsoft EA Agreement (Servers & Security)	**258,000**	48,000	42,000	42,000	42,000	42,000	42,000
Microsoft EA Agreement (Windows & Office)	**1,159,000**	139,000	204,000	204,000	204,000	204,000	204,000
Microsoft EA Agreement (Application Development)	**75,000**	5,000	14,000	14,000	14,000	14,000	14,000
	2,172,000	**265,000**	**354,000**	**262,000**	**562,000**	**467,000**	**262,000**
IT003 ICT Hardware							
Desktops (target 20%)	**251,600**	51,100	40,100	40,100	40,100	40,100	40,100
Laptops/Tablets & Docking Stations (target 20%)	**374,400**	64,400	62,000	62,000	62,000	62,000	62,000
Monitors & Monitor Arms (target 20%)	**84,800**	14,800	14,000	14,000	14,000	14,000	14,000
Peripherals replacement (target 20%)	**18,200**	3,200	3,000	3,000	3,000	3,000	3,000
Mobile device replacement (target 20%)	**21,100**	6,100	3,000	3,000	3,000	3,000	3,000
Replacement Backup Tape Drive	**25,000**			25,000			
IP TV Asset Refresh	**50,000**		25,000	25,000			
Landline Handset Refresh	**10,000**					10,000	
Audio Visual Conference Facility	**120,000**		120,000				
Audio Visual Refresh Stations	**75,000**		75,000				
Audio Visual Refresh TDA	**75,000**	75,000					
	1,105,100	**214,600**	**342,100**	**172,100**	**122,100**	**132,100**	**122,100**
IT005 ICT Servers							
Server/storage replacement (target 20%)	**398,000**	73,000	65,000	65,000	65,000	65,000	65,000
Server/storage growth	**84,000**	14,000	14,000	14,000	14,000	14,000	14,000
SAN 5 Year Refresh	**135,000**						135,000
	617,000	**87,000**	**79,000**	**79,000**	**79,000**	**79,000**	**214,000**
IT018 ICT Network							
Local Area Network replacement (discrete)	**215,000**	215,000					
Network Switches/Router replacement	**82,000**	72,000	2,000	2,000	2,000	2,000	2,000
Network Switches/Routers Growth	**30,000**	5,000	5,000	5,000	5,000	5,000	5,000
Network Data Port Replacement	**50,000**		10,000	10,000	10,000	10,000	10,000
Core Network Switch/Router upgrade	**200,000**						200,000
MDT Wireless Network Replacement	**25,000**						25,000
Public Wi-Fi Replacement	**15,000**						15,000
Vesty Road Network Link Refresh	**80,000**	40,000					40,000
Secondary FireControl backup telephony refresh	**40,000**						40,000
	737,000	**332,000**	**17,000**	**17,000**	**17,000**	**17,000**	**337,000**
IT026 ICT Operational Equipment							
Pagers/Alerters	**98,500**		78,500	5,000	5,000	5,000	5,000
Station Equipment Replacement	**60,000**	10,000	10,000	10,000	10,000	10,000	10,000
Incident Ground Management System	**60,000**	10,000	50,000				
MDT Replacement (Not incl. in ESMCP)	**195,000**		120,000			75,000	
Toughpad 5 Year Asset Refresh	**150,000**						150,000
	563,500	**20,000**	**258,500**	**15,000**	**15,000**	**90,000**	**165,000**
IT058 New Emergency Services Network (ESN)							
ESN Radios / Infrastructure - Estimate	**77,000**	23,000	54,000				
	77,000	**23,000**	**54,000**				
IT060 ICT Station Change							
St Helens Station End Mobilising Equipment	**16,000**	16,000					
	16,000	**16,000**					
Other IT Schemes							
IT019 Website Devolpment	**34,000**	34,000					
IT027 ICT Security - Remote Access Security FOBS	**12,000**	2,000	2,000	2,000	2,000	2,000	2,000
IT028 System Development (Portal)	**124,000**	14,000		110,000			
IT030 ICT Projects/Upgrades	**25,000**		5,000	5,000	5,000	5,000	5,000
IT047 Legal Case Management System	**42,500**	42,500					
IT055 C.3.I. C.&.C Communication & Information System	**25,000**		5,000	5,000	5,000	5,000	5,000
IT056 Door Access System	**9,000**	9,000					
IT057 Fleet Management System	**5,000**	5,000					
IT059 ESMCP Project Control Room Integration	**92,000**	66,000	26,000				
IT061 ESMCP ITHC Remedial Works							
IT062 Capita Vision 3 Update (CFO/058/17)	**950,000**	805,000	145,000				
FIN001 FMIS/Eproc/Payroll/HR Replacement	**254,000**	74,000	180,000				
NEW Planning Intelligence and Performance System (PIPS)							
PIPS System upgrade	**120,000**				120,000		
	1,692,500	**1,051,500**	**363,000**	**122,000**	**132,000**	**12,000**	**12,000**
	6,980,100	**2,009,100**	**1,467,600**	**667,100**	**927,100**	**797,100**	**1,112,100**

Return to Top.

Appendix D – Application Status

Merseyside Fire and Rescue Authority - Applications Status Update

ITIL Standards

New	Conceived, in planning phase, under construction or newly deployed
Emerging	In production or licenses have been purchased, but in limited use, such as a pilot
Mainstream	In production and actively being used
Containment	In production for a specific or limited purpose
Sunset	In production with scheduled retirement in progress
Prohibited	No longer used

Application Name	Function	Status	Contract Renewal Date
pharOS10 Legislative Fire Safety	Protection Department Module of Sophtlogic. The module is fully featured for the support and maintenance activities and records associated with the Protection function. It offers detailed premises record files, full details of inspections and visits, history of all steps within Certification Process and details of legislative events.	Sunset	31/03/2020
Wand/FireSpace	Remote Fire Safety Audit Tool. WAND allows Fire Safety Officers to download Fire Safety Audits, complete them electronically, before synchronising them back to the central FRS MIS database.	Sunset	31/03/2020

Goldmine (Front Range)	This is a CRM application used by Fire Service Direct in the Community Fire Safety arena.	Mainstream	16/06/2020
HFSC App (SharePoint Portal)	InfoPath form used by stations to record and refer home fire safety checks	Containment	N/A
IIT Database	Used by IIT to record and report on data relating to incident investigations	Mainstream	N/A
SOFSA (Simple Operational Fire Safety Assessment)	This is used by Protection Department and Stations for recordings information relating to a Simple Operational Fire Safety assessment.	Mainstream	N/A
Business Objects	A reporting tool used in Finance.	Mainstream	31/08/2023
E-Financials & E-Procurement	Finance, stores and procurement package	Mainstream	31/08/2023
Civica Case Management	Legal case management system includes a library of documents and workflows linked to a central database. Multiple operations and bulk processing are driven from a single input, whilst shared items can be used to store information related to a particular client, matter or case work.	Sunset	26/02/2020
Iken Legal Case Management	Legal case management system includes a library of documents and workflows linked to a central database. Multiple operations and bulk processing are driven from a single input, whilst shared items can be used to store information related to a particular client, matter/case work.	New	29/11/2022
Modern Gov	Committee decisions management system used to manage authority business including ensuring relevant papers are published to members via the MFRA web page.	Mainstream	31/12/2020
Resourcelink	NGA HR and payroll functionality hosted by ABS 365 to manage the entire employee lifecycle from recruitment to staff development, succession planning and payroll.	Mainstream	31/08/2023

Org Plus	Used by People and Organisational Development to produce organisational charts using the data exported from Resourcelink.	Mainstream	N/A
File Director	Scans and organises images of paper documents used in People and Organisational Development.	Mainstream	01/07/2020
PageTiger	Software that ensures new joiners have all the information they need for a productive onboarding.	Mainstream	11/11/2020
Civica Tranman	Vehicle Fleet Management System	Mainstream	30/01/2024
Red Kite	Equipment/asset management system. Used on stations to ensure operational equipment is checked regularly and appropriately maintained.	Mainstream	31/07/2020
Airbus Hydra	GIS (Geographical Information System) solution which provides risk and hydrant data to the incident ground and organisation.	Mainstream	31/05/2020
Draeger	BA (Breathing Apparatus) testing software	Mainstream	07/12/2020
LearnPro (EFS)	eLearning Management Systems provided by eFireService Ltd	Mainstream	30/04/2022
Auto CAD Architecture (Graitec)	CAD (Computer Aided Design) software	Mainstream	06/01/2021
Wall Chart	Training Resource Planner	Mainstream	
SSRI Progress	Captures site specific risk information and presents it to crews via the MDTs.	Containment	N/A
Voyager Fleet	Black box data logger on vehicles.	Mainstream	29/04/2020
CAPITA Vision FX	CAD Computer aided dispatch. This system logs all incoming emergency calls and supports the mobilisation of appropriate resources for incident management. Currently in use within FireControl.	Mainstream	31/03/2020

CAPITA DS3000	ICCS (Integrated Communications & Control System) partnered to the Vision FX CAD System. This system enables FireControl to utilise Radio & Telephony functions to manage incoming 999 calls and communicate with MFRA resources. Currently in use within FireControl.	Mainstream	31/03/2020
SEED Data Mobilisation (BRIGID)	Data Mobilisation: FireControl mobilise crew to incidents by sending a message to the Mobile Data Terminal (MDT) installed in the Appliance. Crews retrieve Risk Related information from the MDT. Currently in use within Operational Vehicles & FireControl.	Sunset	30/06/2020
SAN H 8-port Vortex System	Firelink delivered solution via CCN 239 which allows the CAPITA DS3000 ICCS to connect directly to the Airwave Network for both Voice and Data communication.	Mainstream	31/12/2020
Vision 3 FX BOSS	Management Information: providing senior officers with real time incident information and the organisation with incident history for trend analysis.	Mainstream	31/03/2020
AIRBUS Sc-Response	Data Mobilisation and Operational Risk retrieval. As part of the replacement programme for the existing SEED (BRIGID) system.	New	N/A
Operational Performance System (OPS)	Internally developed SQL based application to allow the detailed recording, monitoring and assessment of fire fighter competencies against national standards for firefighters.	Mainstream	N/A
Resilience Direct	A replacement service for the National Resilience Extranet that can be built upon to provide additional innovative ways to enhance multi-agency working.	Mainstream	N/A
Airbus Steps	Operational Incident Management package installed on devices on the Authority incident management vehicle.	Mainstream	31/05/2020
OSHENS	Health & Safety managfement information system.	Mainstream	31/12/2020

Simul8 - Process Evolution	Fire Incident Response Simulator (FIRS) Fire Incident Analyser (FIA) Facility Location Planner (FLP) Used by Strategy and Performance for operational response planning and modelling.	Mainstream	28/02/2020
Ximes	Shift pattern modeller	Mainstream	18/10/2020
StARS	TRM (Time and Resource Management) staffing system.	Mainstream	31/08/2020
AVCO Anycoms	Middleware which reduces the requirement for manual input and transfers files securely between local authorities.	Mainstream	31/12/2020
Gazetteer	Aligned Assets Gazetteer Application. Corporate gazetteer in use across the Authority to provide standardised address information and UPRN data to corporate systems and users.	Mainstream	28/02/2020
Crystal Reports	Reporting tool used in Strategy and Performance.	Mainstream	N/A
IRS (CLG)	Incident Recording System which interfaces, extracts data from Vision	Mainstream	N/A
Planning, Intelligence and Performance System (PIPs)	System that streamlines and enhances functionality relating to station plans, business intelligence, performance management, GIS plotting, project and risk management.	Mainstream	31/07/2020
Portal	SharePoint Portal is used to provide the corporate intranet and central repository for MFRS core data.	Mainstream	08/11/2020
MapInfo GIS	MapInfo is a geographical information system used within Strategy and Performance to display and analyse geo-spatial datasets.	Mainstream	30/05/2020
Fueltek	Fuel management system	New	31/05/2023
SIRAH (Site Information of Risk and Hazard)	A service wide application used to capture, store and consume all operational risk information.	New	N/A

National Resilience Management System (inc. ESS)	A management system used by the National Resilience Assurance Team (NRAT) and the National Coordination Centre (FRSNCC).	New	N/A
The Hub	Management Information System that provides centralised control and data management of all internally developed mobile apps.	New	N/A
Protection	Mobile application that will be used to collect information at fire safety inspections.	New	N/A
Prevention	Mobile application that will be used to collect information at home fire safety checks and safe and well visits.	New	N/A

Return to Top.