ICT Asset Management Plan

2023 - 2028

Table of Contents

ICT Asset Management Plan

1 Overview

1.1 Information and Communications 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 secure, functional, flexible ICT infrastructure possible and 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 ITIL, can lead to improvements in efficiency, performance and cost management.

ICT can be split into six key delivery areas:

- The ICT infrastructure – data, 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 O365
- Fire Control applications which run on the ICT infrastructure – Vision 5 Computer Aided Dispatch (CAD), Vision 5 BOSS, Airbus ScResponse and staff attendance
- Financial & HR applications which run on the ICT infrastructure – ABS eFinancials, ResourceLink and the Staff Attendance Recording System (S.t.A.R.S)
- Corporate applications that run on the ICT infrastructure – Tranman, Planning Intelligence and Performance System (PIPS), the intranet 'Portal' (SharePoint), and CFRMIS
- 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) or Community Risk Management Plan (CRMP) 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 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.

The introduction of Microsoft System Centre Configuration Manger (SCCM) has seen patching carried out over and above Business as Usual (BAU) activity, because of the ability to automate tasks.

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 has 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, Surface Pros and mobile devices – against viruses, malware, advanced threats and targeted attacks.

Mobile Device Management (MDM) for Samsung mobiles phones is in place, protecting our information more securely than in the past.

MDM is provided by Microsoft Intune 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), the Data Protection Act 2018 (DPA) 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 preventative 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, 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 via a request to ICT.

3.4 Audit

In 2021/2022, internal audit focused on the audit area of 'MFRA Asset Management of ICT Devices and Phones'. The audit objectives were to review the arrangements in place at MFRA for management of ICT devices and phones to obtain assurance on the adequacy and effectiveness of the controls.

The scope of the audit included examining controls relating the following areas:

- Accuracy of the ICT asset register.
- That there is a nominated officer responsible for maintaining the ICT asset register.
- New stock is added to asset register on receipt.
- That there is an effective strategy for refreshing obsolete equipment.
- Obsolete stock is disposed of in line with industry standards and the asset register is updated.
- Assets allocated to staff who leave are returned to ICT, 'wiped' and reused where appropriate.

Findings of the audit will be reviewed at the appropriate S&P ICT Board and any remedial activities will be discussed and approved.

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 – Monthly

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 (MIR) 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 Digital Workplace allows 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 Service Delivery 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 are:

- 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 archives

5.4 Lifecycle Management

The ICT challenge is to provide the most functional, flexible ICT infrastructure possible and to host the applications that deliver benefits to the organisation, all at the lowest cost of ownership. Meeting this 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 quarterly 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 by, 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 Board

There are three thematic S&P boards in place: ICT (with Corporate Information & Systems Manager), Estates, and Performance Planning and Risk Information, which means a thematic S&P ICT Board meets every three months. The purpose of the S&P ICT 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
- Purchasing 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, if there are confirmed performance issues. 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, if there are confirmed performance issues.

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 2022/2023

The key ICT Asset movements to highlight in 2022/2023 are:

MDT rollout to the Reserve Fleet

The rollout of frontline and reserve fleet MDTs has been completed (Panasonic CF33). The rollout of MDTs (Panasonic FZ-G1) to the secondary fleet followed and this was completed in 2021/2022.

WTR alerting

The Whole Time Retained rollout has been successfully completed, with a mix of corporate and personal phones being used with the CallMy solution. Prevention have shown an interest in using CallMy to improve lone worker safety.

GPS Repeaters on Stations

Final completion of the installation and switch on of GPS signal repeaters on Station to allow a quick GPS connection as appliances are mobilised to incidents.

Force Point & Sophos

Force Point (Web Filtering) & Sophos (Anti-virus) contract renewal and a move to using the cloud versions.

Multi-Functional Device Tender

Tender proposals were received from four suppliers. The bids were reviewed and scored, and a paper citing HP as the winning vendor was approved by the Authority on 9th June 2022. Following this, HP Commissioning and Konica decommissioning of devices took place.

Upgrade to Remedy

Telent use the Remedy IT Service Management (ITSM) tool for the Service Desk and other activities. Remedy 9 went live for MFRS, incorporating a new Self Service Portal.

Decommission of Legacy VPN

The introduction of Celestix solution for two factor authentication when accessing the Corporate Network, Making use of a mobile phone app of a physical fob.

Public Wi-Fi

Provision of a new Public Wi Fi 'appliance & firewall' to allow greater scalability as the number of Wi Fi Access points increase and the removal of a cyber security concern.

IP TV Refresh

30 x IPTV receivers have been successfully replaced along with an upgraded Media Gateway providing additional Freeview channels across MFRS sites.

National Resilience (NR) Audio Visual

Provision of CleverTouch room solution and audio visual in the Area Manager's Office.

Return to Top.

7 Fire Control Applications and Hardware Assets

Reporting to the Head of Technology, the Application 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
- Application Life Cycle Management
- 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.

There are six high level areas of ICT in Fire Control.

- Computer Aided Despatch (CAD) - This is where incoming emergency calls are logged, and the appropriate resources mobilised to the incidents. MFRA use the SSS (formally Capita) Vision 5 CAD application implemented in April 2021.
- Management Information System (MIS): providing senior officers with real time incident information and the organisation with incident history for trend analysis. MFRA use the SSS (formally Capita) Vision 5 BOSS.
- 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 and 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.

  An ICCS will work in tandem with a CAD application. The ICCS is the place where incoming emergency calls are answered, and the CAD is where the calls are logged and resources despatched. MFRA use the SSS (formally Capita) Ds3000 ICCS.

- Wide Area Radio Scheme: Emergency services rely on seamless radio communications coverage to effectively perform their daily tasks. MFRA, in keeping with the Police and Ambulance, use Airwave.

  NOTE: The Emergency Services Mobile Communication Programme, (ESMCP) set up by the Home Office, aims to replace the current communication service provided by Airwave. The new service will be delivered across the Emergency Services Network (ESN) and MFRA will connect to this network via a Direct Network Service Provider (DNSP). At present, however, all individual FRS activities for this project have been suspend.

- Data Mobilisation: Fire Control can mobilise crews to incidents by sending a message to the Mobile Data Terminal (MDT) installed in the appliance. MFRA use Mobile Data terminals running ScResponse from Airbus.

- Station-End Turnout: Various hardware and software components and subsystems are installed in every Merseyside Fire Community Fire Station. 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. MFRA utilise station-end Firecoders from Multitone Electronics.

7.2 Fire Control ICT Project Review

Computer Aided Despatch and Management Information System (CAD-MIS) is a series of projects where ICT has delivered, and will continue to deliver, improvements for Fire Control.

CAD-MIS Phase One

CAD-MIS Phase One: In September 2017, the Authority approved a project to replace Vision 3 FX CAD & Vision 3 MIS with 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.

The implementation of Vision 5 went live on 21st April 2021 and a period of early life support followed. Vision 5 will assist in our duty to respond to all emergency calls with a level of response appropriate to the risk, and deal with all emergencies efficiently and effectively.

CAD-MIS Phase Two

Following successful completion of Phase One activities, a prioritised list of Phase Two activities was finalised and approved. What follows is an update on the activities chosen:

- ESN Ready & DCS - The upgrade of the end-of-life Airwave equipment to the new Dispatch Communication Server (DCS) is ongoing and aligned to ICCS technical refresh activities. Airwave has installed the dedicated fibre at SHQ and the upgrades to core equipment and Fire Control operator positions are progressing. Following the Home Office announcement that the Emergency Services Network (ESN) will be suspended for 18-24 months from March 2023, the ESN Solution Deployment project (CCN1045) has been closed following discussions with suppliers.

- Dynamic Cover Tool – The MFRS internal development team have produced a new application called AURA, which satisfies all the minimum requirements highlighted. The software has now been made available for testing in Fire Control and the training room. Feedback will inform any future changes to the product including plans for moving from test to the live environment.

- Fire Survival Guide – An internal solution has been produced which has been implemented into Fire Control and satisfies minimum requirements. Investigations continue to explore options for an integrated solution.

CAD-MIS Phase Three

Mindful of the requirement to maintain the appropriate lifecycle management of hardware and software applications, there is a need to consider a series of related phase three activities including:

- Utilisation of the Pre-Alert function within the Vision 5 CAD.

- The potential extended use and maintenance of Airwave, associated with any ECSMP suspension of activities.

Post CAD-MIS Phase Three

Following CAD-MIS Phase Three, the Authority will be in a strong position to take stock and assess the introduction of the next generation of Fire Control Command & Control solutions.

This requirement has been Identified within the Five-Year ICT Capital Plan Commentary stating that the existing Vision 5 and the Ds3000 ICCS will need replacing circa 2027/2028 at an estimated cost of £2m and that work on a separate business case is recommended to commence in April 2024-2025.

7.3 Emergency Services Network (ESN*)*

In December 2021 the Authority approved ICT Capital budget growth of £770k for ICT to deliver the three elements for MFRS to become ESN Ready and maintain existing use of Airwave.

The resulting projects being:

- ESN Solution Deployment
- Ds3000 Technical Refresh
- Dispatch Communications Server (DCS) Install

However, following the early departure of Motorola from the ESMCP programme in December 2022, the Home Office have commenced a re-procurement exercise for a replacement Lot 2 supplier / Prime Contractor.

The Home Office have therefore agreed to suspend all ESN related activities from March 2023 for a period of 12 – 18 months or until such time that the re-procurement exercise completes.

Assurance Partner activities will therefore cease after March 2023 and the Home Office have thanked MFRS for the work and effort undertaken in testing the associated products and delivering many of the key project milestones.

The consequences of the ESN suspension are that whilst the Ds3000 Technical Refresh and DCS Install projects will continue and complete during 2023, the ESN Solution Deployment project will terminate with immediate effect.

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.

To continue to use the latest versions of Microsoft products, such as Window Server, Windows 10, Windows 11 and O365, MFRA has a Microsoft Enterprise Agreement (EA) for the majority of its Microsoft software licences.

In 2023/2024 the MFRS Microsoft EA expires, and it will be renewed under the Crown Commercial Services (CCS) Digital Transformation Agreement 2021 (DTA21).

The DTA21 runs till April 2024, and it is a Memorandum of Understanding (MOU) between the UK Government and Microsoft to enable public sector organisations to continue to unlock the benefits of cloud computing and business applications

Under the EA, Microsoft has bundled together Windows, Office 365 and a variety of management tools to create a subscription suite: Microsoft 365 (M365). MFRA is licensed for M365 and this has allows ICT to deploy Microsoft Teams.

At the same time as the renewal, MFRS will award a three-year contact to a Microsoft Licensing Solution Partner (LSP). A LSP provides information and guidance about contacting, identifying, and choosing Microsoft licencing.

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 three to five year lifecycle and, prior to any future renewal, a fit-for-purpose exercise and market evaluation 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 is 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 that 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
SSRI Progress	Mainstream
National Resilience Application	Mainstream
Merseyside Fire & Rescue Service Website	Mainstream
AURA	New

9.5 Financial Implications of New or Replacement Applications

The requirement for new or replacement applications is monitored throughout the year and will follow the application governance process outlined in sections 9.2 and 9.3 of this document.

There will be one large scale application project undertaken during this five-year period, and capital reserves have been identified and put in place to support this project. The Finance, HR and time and resource management applications are due for replacement within the next two years and a provision of £254K has been included in the 5 year ICT capital programme plus £300k in the capital reserve.

In addition to the above, there has been budget allocated in the ICT capital programme to fund other applications that are planned for the next five years.

The application portfolio will be kept under review and requests for additional capital or revenue will be submitted if required. It is not envisaged that they will be significant amounts.

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 & CRMP Project Spend	Spend on specific IRMP or CRMP projects where ICT is a major enabler e.g. station change	This spend delivers the Authority's IRMP or CRMP	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 2023/2028 Five-Year Capital Plan can be found in Appendix C – 2023/2028 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-premises, 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 transition over the coming years.

Return to Top.

11 Glossary

ABR	Asset Based Resourcing
AES	Advanced Encryption Standard
ALM	Application Lifecycle Management
AP	Assurance Partner
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
CFRMIS	Community Fire Risk Management Information System
CMS	Configuration Management System
CoCo	Code of Connection
CRMP	Community Risk Management Plan
CSI	Continuous Service Improvement
CTA	Cloud Transformation Agreement
DCS	Dispatch Communications Server
DML	Definitive Media Library (previously Definitive Software Library, DSL)
DNSP	Direct Network Service Provider
DPA	Data Protection Act
DTA	Digital Transformation Arrangement
ED&I	Equality, Diversity and Inclusion
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
GPS	Global Positioning System
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
MIR	Major Incident Report
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
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
CAD Servers – Tier 1 (≤£5000)	17
CAD Servers – Tier 2 (≥£5000)	0
CAD Desktops	32
CAD Monitors	52
ICCS Servers	1
ICCS Clients	20
ICCS Touchscreen	20
ICCS Capita VAIU	20
Fire Control Headsets	40
Airwave SAN H Radio Gateway	1
Alerter Masts	4
UHF Radio Packsets	632
Station End Firecoders	27
Station End Turnout Printers	32
Station End Auxiliary Relay Unit (ARU)	32
Station End Amplifiers	34
Station End UPS	40
Modems	63
Mobile Data Terminals	43
Airwave Radio SAN A	112
Airwave Radio SAN B	10
Airwave Radio SAN J	80

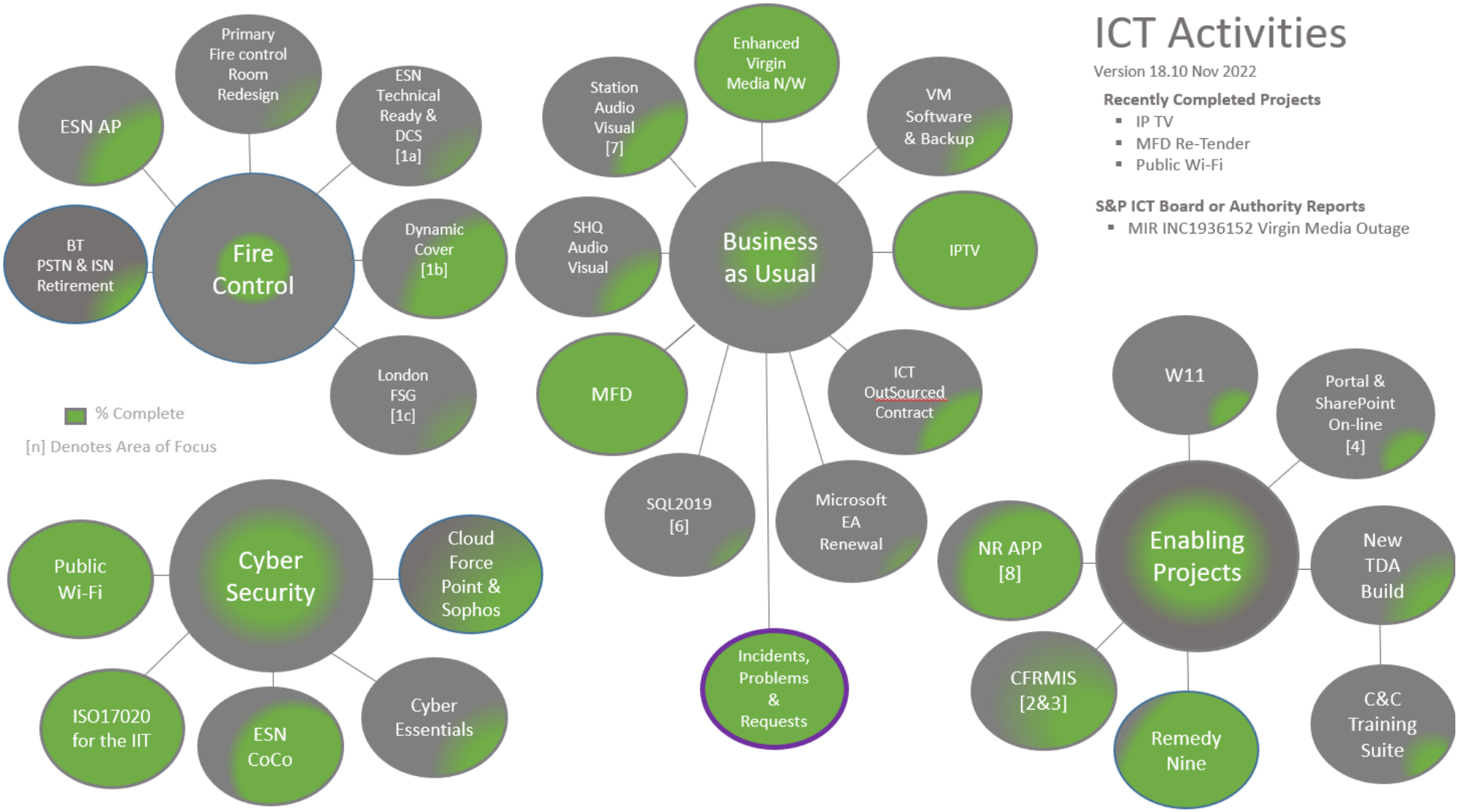
Administration Infrastructure, Managed Servers & Desktop	Quantity
Servers – Tier 1 (≤£5000)	39
Servers – Tier 2 (≥£5000)	3
HPE Modular Storage Arrays (MSA)	3
HPE Storage Shelves	8
HPE Tape Library	1
Desktops	312
Laptops	26
Microsoft Surface Pro	350
Microsoft Surface Laptop	111
Microsoft Surface Book	15
Microsoft Surface Go	14
Panasonic Toughpads	99
Docking Stations (Laptops & Surface Devices)	645
Docking Stations (Toughpads)	186
Monitors	1146
Non-Standard Printers (Additional to leased HP devices)	9

HP Multi-Function Devices	53
HP Desktop Print Devices	10
Security Appliance – Tier 1 (≤£2000)	5
Security Appliance – Tier 2 (≥£2000)	5
Router – Tier 1 (≤£2000)	10
Router – Tier 2 (≥£2000)	26
Switch – Tier 1 (≤£2000)	31
Switch – Tier 2 (≥£2000)	56
Wireless Controller	1
Wireless Access Points	90
Mitel IP Sets	674
Mitel Conference Unit	12
Ubiquiti Nanobeam Wireless Bridge	2
SIKLU Radio Link	6

Miscellaneous	Quantity
Smartphones (Samsung)	364
iPhones	8
Non-Smartphones (Alcatel/Nokia)	517
MTPAS Enabled Mobile SIMS	104
MDT Enabled Data SIMS	42
iPads	13
Encrypted USB devices	141
3G/4G Dongles	33
Battery Chargers	137
Projectors (includes Smartboards)	45
Barco Click Share	11
Display Screens	29
Clevertouch Screen	4
IPTV - Gateways	1
IPTV - Receivers	30
Remote Access Tokens (Celestix)	169
Running Call Phones	24

Return to Top.

Appendix B – Key ICT Projects and Activities (S&P ICT Board 18/11/2022)



Highlighted Business as Usual (BAU)

Item	Description	Status
Incidents, Problems & Requests	These are the day-to-day disruptions to the ICT BAU Services. e.g. loss of internet, e-mail.	None since last meeting.
Enhanced Virgin Media Network	Upgrade of network connections to all MFRS sites.	Project is completed. Follow on activity is a 1gb upgrade of the SHQ internet connection and the replacement of users stacks and core switches.
Station Audio Visual	The replacement of existing projectors and smartboards with new Clevertouch Screens & 75 inch TVs, at non-PFI stations only.	Same as Areas of Focus.
Public Wi-Fi	Provision of a new Public Wi Fi *'appliance & firewall'* to allow greater scalability as the number of Wi Fi Access points increase.	Project is completed and it removes a cyber security concern. Follow on activity is to order new Wi-Fi access Points.
MFD Re-tender	The re-tender of the Multi Functional Device (MFD) contract, which expired July 2022.	Project is completed. The final phase of this project was the rollout of Apogee/HP MFDs to the whole MFRS estate. The new contract will expire in July 2027.
IPTV Refresh	The hardware that currently serves IPTV for 30 TVs across MFRS sites is now end of life and requires replacing.	30 x IPTV receivers have been successfully replaced along with an upgraded Media Gateway providing additional Freeview channels across MFRS sites.
Microsoft EA Renewal	To continue to use the latest versions of Microsoft products such as Window Server, Windows 11 and O365, MFRS will need to renew its Microsoft Enterprise Agreement (EA), which expiries 31/03/2023.	Initial preparatory meetings are taking place between Crown Commercial Service (CSS), Procurement and ICT. The current cost of the Microsoft EA is £250k.
Windows 11	On 5th October 2021 Microsoft announced it will be replacing Windows 10 with Windows 11.	Windows 11: a watching brief is in place.

Highlighted Projects

Item	Description	Status
ESN Technical Ready & DCS	Dispatch Communication Server (DCS) - Replacement of end-of-life SAN H Airwave equipment with a DCS solution. Fire Control fully integrated into the Emergency Services Network (ESN).	The projects to deliver DCS and the ICCS tech refresh continue with a project board in place and meeting regularly. The scope is being finalised to take into account changes mandated by Motorola for DCS and the hardware for the tech refresh is expected onsite at SHQ towards the end of the year for implementation at a time agreed with Fire Control. *(Verbal up date on other ESN activities on the Agenda).*
Cyber Essentials	Cyber Essentials is a simple but effective, government-backed scheme that helps to protect organisations, whatever their size, against a whole range of the most common cyber attacks.	This project involves Telent, Telent's cyber security partner Aristi, and MFRS. A meeting will take place w/c 14/11/2022 to pull together various work streams to complete the pre-assessment questionnaire.
New TDA	ICT for the new TDA, the station, Secondary Fire Control and C&C Training Suite.	Stage 4 design works - ICT is liaising with Estates, Wates and stakeholders, and weekly meetings are now in place.
BT PSTN & ISN Retirement	In 2025 the last elements of Openreach's analogue and digital ISDN copper network will be turned off as an all-IP network replaces these legacy services. The impact on telephony and broadband services is far-reaching and it will affect the 999's	LFB, Surrey and Yorkshire FRS are testing SIP for their 999s. The Cradle Point solution for secondary appliance mobilisation on Station. BT have offered to survey 10 stations free of charge and this offer is likely to be taken up.
Virtual Servers & Backup	New virtualisation and backup solution to will improve the system's resilience and business continuity and disaster recovery options, allowing servers to be easily replicated between SHQ and TDA.	Telent have been working with a Technical Solutions Architect to produce a high level design for new solution along with hardware and software quotes. Quotes are now under review.
Upgrade to Remedy 9	Telent use the Remedy IT Service Management (ITSM) tool for the Service Desk and other activities.	The Self-Service Portal went live June 2022. Follow on steps: Migration of CMDB and integration into ResourceLink.

Return to Top.

Appendix C 2023/24 – 2027/2028 ICT Five Year Capital Plan

ICT Capital Programme 2023/24 to 2027/28

Type of Capital Expenditure	Total Cost £	2023/24 £	2024/25 £	2025/26 £	2026/27 £	2027/28 £
IT002 ICT Software						
Software Licences	10,000	2,000	2,000	2,000	2,000	2,000
New Virtualisation Infrastructure	75,000	75,000				
5 Year Antivirus & Filtering Software	20,300	20,300				
MDT Software Solution Refresh	100,000	100,000				
Microsoft SQL Upgrade	50,000	50,000				
Logpoint Security Information and Event Mgmt (SIEM)	206,000	103,000			103,000	
3 Year Antivirus & Filtering Software	150,000			150,000		
3 Year PRTG Subscription License	6,000			6,000		
Microsoft EA Agreement (Servers & Security)	155,000	31,000	31,000	31,000	31,000	31,000
Microsoft EA Agreement (Windows & Office)	1,210,000	242,000	242,000	242,000	242,000	242,000
Microsoft EA Agreement (Application Development)	185,000	37,000	37,000	37,000	37,000	37,000
	2,167,300	660,300	312,000	468,000	415,000	312,000
IT003 ICT Hardware						
Desktops (target 20%)	228,300	44,200	40,100	48,000	48,000	48,000
Laptops/Surface Pros/Tablets/Docking Stations (target 20%)	489,600	66,100	62,000	120,500	120,500	120,500
Monitors & Monitor Arms (target 20%)	74,100	18,100	14,000	14,000	14,000	14,000
Peripherals replacement (target 20%)	15,000	3,000	3,000	3,000	3,000	3,000
Mobile device replacement (target 20%)	66,340	16,860	12,360	12,360	12,360	12,400
Mitel Handset Refresh	135,000					135,000
Replacement Backup Tape Drive						
IP TV Asset Refresh						
Landline Handset Refresh	10,000	10,000				
Audio Visual Conference Facility - SHQ	64,100	4,100	60,000			
Audio Visual Conference Facility - TDA						
Audio Visual Conference Facility - Stations	4,100	4,100				
New TDA site						
New Long Lane Station	22,400	22,400				
Backup Tape Drive 5-year asset refresh	25,000				25,000	
IPTV 5-year asset refresh	36,800				36,800	
Members Push Button Microphone replacement	25,000	25,000				
	1,195,740	213,860	191,460	197,860	259,660	332,900
IT005 ICT Servers						
Server/storage replacement (target 20%)	555,600	295,600	65,000	65,000	65,000	65,000
Server/storage growth	84,000	28,000	14,000	14,000	14,000	14,000
SAN 5 Year Refresh	135,000		135,000			
	774,600	323,600	214,000	79,000	79,000	79,000
IT018 ICT Network						
Local Area Network replacement (discrete)						
Network Switches/Router replacement	10,000	2,000	2,000	2,000	2,000	2,000
Network Switches/Routers Growth	25,000	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	242,900	42,900	200,000			
Wireless Access Points and Wireless Controllers - Increase	74,500	74,500				
MDT Wireless Network Replacement	50,000		25,000	25,000		
Public Wi-Fi Replacement	15,000		15,000			
Vesty Road Network Link Refresh	40,000		40,000			
Secondary FireControl backup telephony refresh	40,000		40,000			
PSTN replacement asset refresh	125,000				125,000	
Enhanced Virgin Media Network Phase Five Wireless Access P	150,000					150,000
	822,400	134,400	337,000	42,000	142,000	167,000
IT026 ICT Operational Equipment						
Pagers/Alerters	20,000	4,000	4,000	4,000	4,000	4,000
Callmy Alert	5,000	1,000	1,000	1,000	1,000	1,000
Station Equipment Replacement	50,000	10,000	10,000	10,000	10,000	10,000
GPS Repeater 5-year asset refresh	55,000					55,000
Toughpad Asset Refresh - Vehicles	150,000		150,000			
MDT Replacement (Not incl. in ESMCP)	75,000	75,000				
NEW Station End Network Equipment Asset Refresh	140,000			140,000		
Increase in Appliances - Equipment	25,400	25,400				
ICU existing hardware 5-year asset refresh	20,000				20,000	
MDT (Screen & CPU) Front Line Vehicles asset refresh	210,000				210,000	
Bromborough Station Refurbishment	30,000	30,000				
	780,400	145,400	165,000	155,000	245,000	70,000

Continued Next Page.

Appendix C 2023/24 – 2027/2028 ICT Five Year Capital Plan - Continued

Type of Capital Expenditure	Total Cost £	2023/24 £	2024/25 £	2025/26 £	2026/27 £	2027/28 £
IT002 ICT Software						
Software Licences	**10,000**	2,000	2,000	2,000	2,000	2,000
New Virtualisation Infrastructure	**75,000**	75,000				
5 Year Antivirus & Filtering Software	**20,300**	20,300				
MDT Software Solution Refresh	**100,000**	100,000				
Microsoft SQL Upgrade	**50,000**	50,000				
Logpoint Security Information and Event Mgmt (SIEM)	**206,000**	103,000			103,000	
3 Year Antivirus & Filtering Software	**150,000**			150,000		
3 Year PRTG Subscription License	**6,000**			6,000		
Microsoft EA Agreement (Servers & Security)	**155,000**	31,000	31,000	31,000	31,000	31,000
Microsoft EA Agreement (Windows & Office)	**1,210,000**	242,000	242,000	242,000	242,000	242,000
Microsoft EA Agreement (Application Development)	**185,000**	37,000	37,000	37,000	37,000	37,000
	2,167,300	**660,300**	**312,000**	**468,000**	**415,000**	**312,000**
IT003 ICT Hardware						
Desktops (target 20%)	**228,300**	44,200	40,100	48,000	48,000	48,000
Laptops/Surface Pros/Tablets/Docking Stations (target 20%)	**489,600**	66,100	62,000	120,500	120,500	120,500
Monitors & Monitor Arms (target 20%)	**74,100**	18,100	14,000	14,000	14,000	14,000
Peripherals replacement (target 20%)	**15,000**	3,000	3,000	3,000	3,000	3,000
Mobile device replacement (target 20%)	**66,340**	16,860	12,360	12,360	12,360	12,400
Mitel Handset Refresh	**135,000**					135,000
Landline Handset Refresh	**10,000**	10,000				
Audio Visual Conference Facility - SHQ	**64,100**	4,100	60,000			
Audio Visual Conference Facility - TDA						
Audio Visual Conference Facility - Stations	**4,100**	4,100				
New Long Lane Station	**22,400**	22,400				
Backup Tape Drive 5-year asset refresh	**25,000**				25,000	
IPTV 5-year asset refresh	**36,800**				36,800	
Members Push Button Microphone replacement	**25,000**	25,000				
	1,195,740	**213,860**	**191,460**	**197,860**	**259,660**	**332,900**
IT005 ICT Servers						
Server/storage replacement (target 20%)	**555,600**	295,600	65,000	65,000	65,000	65,000
Server/storage growth	**84,000**	28,000	14,000	14,000	14,000	14,000
SAN 5 Year Refresh	**135,000**		135,000			
	774,600	**323,600**	**214,000**	**79,000**	**79,000**	**79,000**
IT018 ICT Network						
Local Area Network replacement (discrete)						
Network Switches/Router replacement	**10,000**	2,000	2,000	2,000	2,000	2,000
Network Switches/Routers Growth	**25,000**	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	**242,900**	42,900	200,000			
Wireless Access Points and Wireless Controllers - Increase	**74,500**	74,500				
MDT Wireless Network Replacement	**50,000**			50,000		
Public Wi-Fi Replacement	**15,000**		15,000			
Vesty Road Network Link Refresh	**40,000**		40,000			
Secondary FireControl backup telephony refresh	**40,000**		40,000			
PSTN replacement asset refresh	**125,000**				125,000	
Enhanced Virgin Media Network Phase Five Wireless Access Points	**150,000**					150,000
	822,400	**134,400**	**312,000**	**67,000**	**142,000**	**167,000**
IT026 ICT Operational Equipment						
Pagers/Alerters	**20,000**	4,000	4,000	4,000	4,000	4,000
Callmy Alert	**5,000**	1,000	1,000	1,000	1,000	1,000
Station Equipment Replacement	**50,000**	10,000	10,000	10,000	10,000	10,000
GPS Repeater 5-year asset refresh	**55,000**					55,000
Toughpad Asset Refresh - Vehicles	**150,000**		150,000			
MDT Replacement (Not incl. in ESMCP)	**75,000**	75,000				
NEW Station End Network Equipment Asset Refresh	**140,000**			140,000		
Increase in Appliances - Equipment	**25,400**	25,400				
ICU existing hardware 5-year asset refresh	**20,000**				20,000	
MDT (Screen & CPU) Front Line Vehicles asset refresh	**210,000**				210,000	
Bromborough Station Refurbishment	**30,000**	30,000				
	780,400	**145,400**	**165,000**	**155,000**	**245,000**	**70,000**
IT027 ICT Security						
Remote Access Security FOBS	**10,000**	2,000	2,000	2,000	2,000	2,000
Celestix 3-year renewal - VPN tokens	**44,000**	22,000			22,000	
	54,000	**24,000**	**2,000**	**2,000**	**24,000**	**2,000**
IT058 New Emergency Services Network (ESN)						
ESN Radios / Infrastructure - Estimate	**40,000**	40,000				
	40,000	**40,000**				
IT063 Planning Intelligence and Performance System						
PIPS System upgrade	**120,000**	120,000				
	120,000	**120,000**				
Other IT Schemes						
IT019 Website Development	**40,000**			40,000		
IT028 System Development (Portal)						
IT030 ICT Projects/Upgrades	**25,000**	5,000	5,000	5,000	5,000	5,000
IT055 C.3.I. C.&.C Communication & Information	**25,000**	5,000	5,000	5,000	5,000	5,000
IT059 ESMCP Project Control Room Integration						
IT062 Capita Vision 3 Update (CFO/058/17)	**25,900**	25,900				
IT064 999 Emergency Streaming (999EYE)	**40,000**	40,000				
IT065 Dynamic Cover/Response Tool	**35,000**	35,000				
IT066 ESN Ready						
IT067 DCS Upgrade						
IT068 Command & Control Suite	**501,000**	501,000				
FIN001 FMIS/Eproc/Payroll/HR Replacement	**253,500**	253,500				
	945,400	**865,400**	**10,000**	**50,000**	**10,000**	**10,000**
	6,899,840	**2,526,960**	**1,206,460**	**1,018,860**	**1,174,660**	**972,900**

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.	Prohibited	N/A
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.	Prohibited	N/A

Goldmine (Front Range)	This is a CRM application used by Fire Service Direct in the Community Fire Safety arena.	Prohibited	N/A
HFSC App (SharePoint Portal)	InfoPath form used by stations to record and refer home fire safety checks	Prohibited	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.	Prohibited	N/A
Business Objects	A reporting tool used in Finance.	Mainstream	31/08/2024
E-Financials & E-Procurement	Finance, stores and procurement package	Mainstream	31/08/2024
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.	Mainstream	29/11/2023
Civica 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	31/12/2023
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	31/08/2024
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	01/07/2023

PageTiger	Software that ensures new joiners have all the information they need for a productive onboarding.	Mainstream	11/11/2023
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	31/07/2023
Airbus Hydra	Water management solution that manages data relating to hydrants.	Mainstream	31/05/2023
Draeger	BA (Breathing Apparatus) testing software	Mainstream	24/02/2024
LearnPro (EFS)	eLearning Management Systems provided by eFireService Ltd	Mainstream	30/04/2023
XVR Simulation	Virtual reality incident command training software for emergency services.	Mainstream	24/05/2023
Auto CAD Architecture (Graitec)	CAD (Computer Aided Design) software	Mainstream	06/01/2024
Timewatch PLC – White Space	Training Resource Planner	Mainstream	31/08/2023
SSRI Progress	Captures site specific risk information and presents it to crews via the MDTs.	Mainstream	N/A
Voyager Fleet	Black box data logger on vehicles.	Mainstream	29/04/2023
CAPITA Vision 5	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	31/03/2024

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	31/03/2024
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.	Prohibited	N/A
SAN H 8-port	Firelink delivered solution via CCN 239 that allows the CAPITA DS3000 ICCS to connect directly to the Airwave Network for both Voice and Data communication.	Mainstream	Rolling monthly renewal until ESN completed
Vision 5 BOSS	Management Information: providing senior officers with real time incident information and the organisation with incident history for trend analysis.	Mainstream	31/03/2024
AIRBUS Sc-Response	Data Mobilisation and Operational Risk retrieval. As part of the replacement programme for the existing SEED (BRIGID) system.	Mainstream	31/08/2025
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.	Prohibited	N/A
OSHENS	Health & Safety management information system.	Mainstream	31/12/2023
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	28/02/2023
Ximes	Shift pattern modeller	Mainstream	18/10/2023
StARS	TRM (Time and Resource Management) staffing system.	Mainstream	28/09/2024
AVCO Anycoms	Middleware that reduces the requirement for manual input and transfers files securely between local authorities.	Prohibited	N/A
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	25/02/2023
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
InPhase - 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	13/07/2023
Silversands – SharePoint Support	SharePoint Portal is used to provide the corporate intranet and central repository for MFRA core data.	Mainstream	26/01/2024

MapInfo GIS	MapInfo is a geographical information system used within Strategy and Performance to display and analyse geo-spatial datasets.	Mainstream	30/05/2023
Fueltek	Fuel management system	Mainstream	31/05/2023
HR Solutions Hub – Firefighter Sift Tool	Online assessment and sift tool for Firefighter recruitment	Mainstream	31/12/2022
ProContract - Proactis	An online Portal for managing the processes around e-tendering and contracts.	Mainstream	31/03/2024
National Resilience Management System (inc. ESS)	A management system used by the National Resilience Assurance Team (NRAT) and the National Coordination Centre (FRSNCC).	Mainstream	N/A
Civica CFRMIS (Community Fire Risk Management Information System)	An application used to collect and manage information relating to Protection, Prevention and Preparedness. All information will be stored in a single database and shared between the three functions.	Mainstream	16/12/2023
Effective Command – K Lamb Associates	The Effective Command™ tool collates data using 3 different applications: Training, Incident Monitoring and Formal Assessment.	New	31/03/2023
AURA	An application produced by our internal development team that displays real-time locations and response coverage of MFRS appliances.	New	N/A

Return to Top.