ICT Asset Management Plan

2019 - 2024

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 - SQL, Oracle, Microsoft Office and e-mail
- Fire Control applications which run on the ICT infrastructure - Vision FX CAD, Vision FX BOSS, SEED and 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, PIPS, the intranet 'portal', SOFSA, 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 - 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 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 the 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.

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.

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, i-Pads 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 of 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 Strategy and Performance (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

The plan is to have thematic S&P boards: ICT & IM (with Finance and System Support); Equality and Diversity (E&D); 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 maintain and develop 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 set 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 Fire Control Applications and Infrastructure 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

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 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 and the Authority has a Capita DS3000. All communications that go into the control room such as 999 telephony calls, administration telephony calls, radio communication and CCTV, plug in to the ICCS. The control room staff then can manage these communications by accessing the ICCS from one place on their desktop

- 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) which 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 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

CAD-MIS Upgrade

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

At the CAD-MIS project board of 02/11/2018, telent presented a proposal which included Rough Order of Magnitude (ROM) costs from Capita to upgrade to Vision5 from Vision 3. The functionality for Vision 5 is defined within a Functional Design Specification (FDS) document which outlines what we will receive for our money. The budgetary price for the 'out of the box' solution is £750k, which also includes associated hardware. Further estimated budget for risk critical enhancements brings the estimated total to £950k to cover all eventualities.

By mid-2019 to end-2019, with the upgrade to Vision 5 complete, the position will be to take stock and determine what will be the Authority's next generation Fire Control solution 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.

ESN

In 2017/2018 a new capital scheme (IT058) was raised to cover the ESN future costs. This is additional to the capital schemes that have been set up to facilitate the Home Office funded preparation works.

Future revenue costs for ESN, which is set for an implementation date of 2021/2022, remain unclear. ESN is rumoured to be 50% cheaper than Airwave which it replaces, however, the grant received from the Home Office is 50% of the current Airwave bill.

Therefore, the current forecast for future revenue spend once implemented, remains neutral.

Future additional costs, however, should not be ruled out at this stage.

6.4 ICT Infrastructure 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.

6.5 ICT Commodity Application Assets

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.

6.5.1 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 and Office, the Authority renewed its Microsoft EA in April 2017, for a further three years.

In 2021/2022 the Microsoft EA expires and will be replaced by the Crown Commercial Services (CCS) Cloud Transformation Agreement (CTA). This will have an effect on the budget, but implications are unknown as commercial discussions have yet to commence.

6.5.2 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.

6.6 Corporate and Financial Application Software

The ICT BRM, as well as acting as the liaison between ICT and the organisation, has a key role to work with System Support, aligning their corporate ALM to the ICT infrastructure, and with Finance to align theirs.

Going forward, from 2020 it is proposed that the overall asset management plan be amended to include the asset management plans for the two departments mentioned.

6.7 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 also 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.

6.8 ICT Asset Movements 2018/2019

The key ICT assets movements to highlight in 2018/2019 are:

- The procurement and initial rollout of 58 Panasonic Toughpads to replace the Panasonic Toughbooks which have reached end-of-life
- The procurement and initial rollout of 120 Surface Pro tablets in line with RBR
- The procurement and commissioning of a replacement WAN solution for the Vesty campus
- Procurement of Multitone equipment to replace existing Station End turnout PCs
- Prescot Community Fire Station go-live, complete with an ICT asset refresh
- A full technical refresh of the Fire Control ICCS which was paid for by Home Office funding (ESN Phase1 Control Room Works)

- A new public Wi-Fi solution along with an increased number of Wi-Fi access points across the MFRA estate

Return to Top.

7 ICT Asset Capital Spend Strategy

7.1 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. Emergency Services Mobile Communications Programme (ESMCP)	Spend to align the Authority's systems to national initiatives	Protecting public safety and increasing national resilience

The 2019/2024 Five-Year Capital Plan can be found in Appendix C – 2019/2024 ICT Five Year Capital Plan

7.2 Review of the Current Capital Programme

In June 2018 ICT carried out a full review of its capital budget in line with the Treasurer's review of the capital programme. The basis for review was 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., or
- Anything else that 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.

7.3 Capital Budget External to ICT

The budget for the replacement and the support of audio visual (AV) equipment on stations and at the Training and Development Academy (TDA) has never been the responsibility of ICT. With the recent extension of the telent contract for a further three years, there is an opportunity for telent to provide first and second line support and, on the Authority's behalf, engage a sub-contractor to provide third line support, for the audio visuals on stations and at the TDA.

If there is an appetite to move the responsibility for the purchase and support of AV equipment on stations and at the TDA to ICT, there is a requirement to provide ICT with the capital to do so. A project is planned for the new year to carry out due diligence in terms of the AV equipment in use and the future requirement of AV across all stations and the TDA.

This has been raised in the 2019/2024 ICT five-Year capital planning process.

7.4 The Emergence of Cloud Computing.

The move to the Cloud and taking ICT as a service, rather than buying a product and installing it on your own ICT equipment, moves the cost of ICT from being mostly a capital, one-off cost to an ongoing 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 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.

8 Glossary

ABR	Asset Based Resourcing
AES	Advanced Encryption Standard
ALM	Application Lifecycle Management
ATF	Authorised Treatment Facility
AV	Audio visual
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 Services
CMS	Configuration Management System
CSI	Continuous Service Improvement
CTA	Cloud Transformation Agreement
DML	Definitive Media Library (previously Definitive Software Library, DSL)
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
ICCS	Integrated Communications Control System
ICT	Information and Communication Technology
ILM	Infrastructure Lifecycle Management
IRMP	Integrated Risk Management Plan
ITAM	IT (or ICT) Asset Management
ITIL	Information Technology Infrastructure Library
LAN	Local Area Network
MDM	Mobile Device Management
MDT	Mobile Data Terminal
MFD	Multi-Function Device
MIS	Management Information System
PC	Personal Computer
PIPS	Planning Intelligence and Performance System
PSG	Protective Security Group
RBR	Role Based Resourcing
S&P	Strategy and Performance
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	27
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	12
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 Mobilising Processors	26
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	136
Mobile Data Terminal touchscreen	98
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

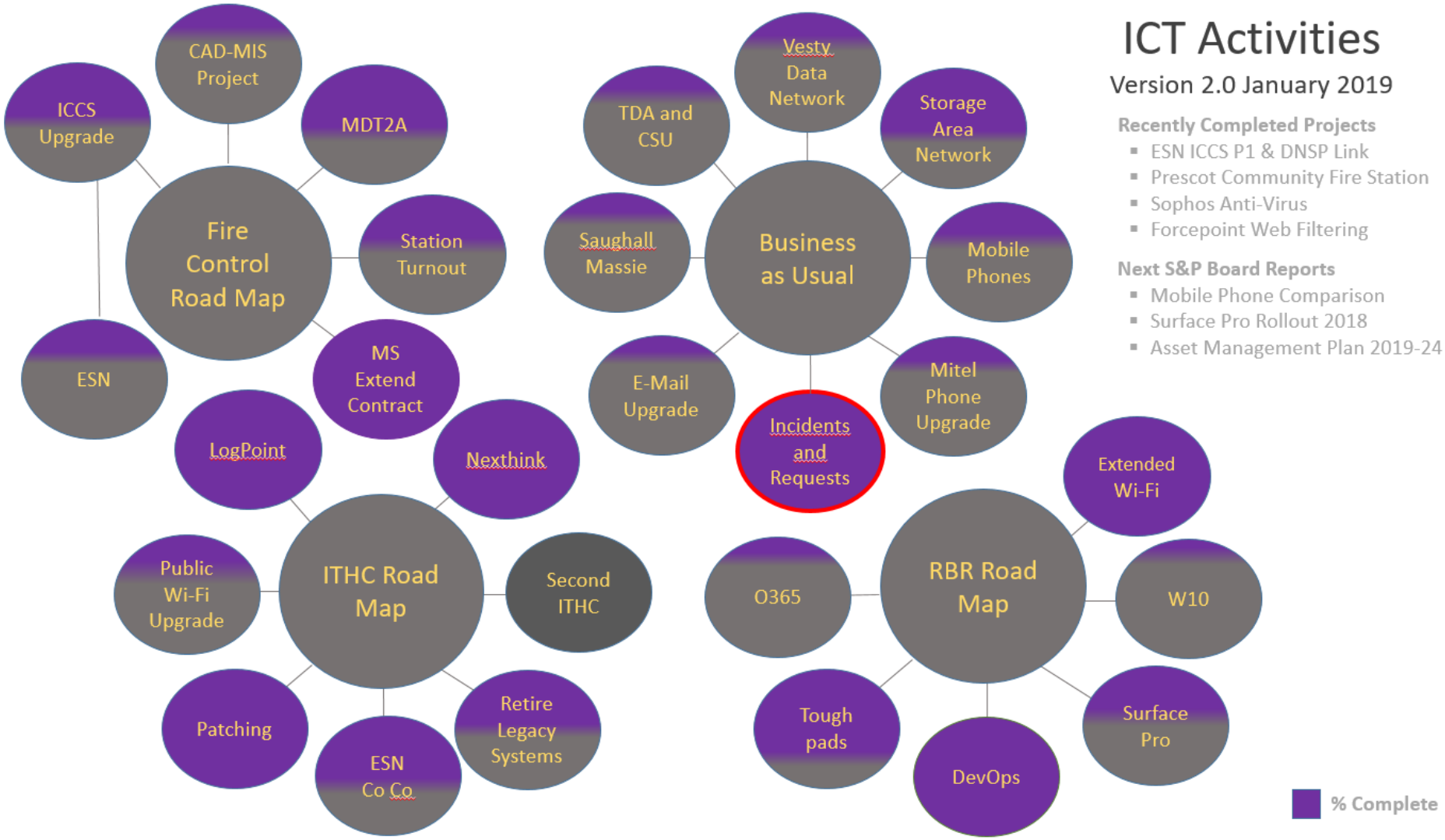
Administration Infrastructure, Managed Servers & Desktop	Quantity
Physical Servers	68
Virtual Servers	102
Desktops *(A limited number of users have two monitors*)	617
Laptops *(Most People have an external monitor)*	376
Docking Stations (Most Laptop Users have an external monitor)	385
Tough Books	60
Monitors	967
HP Printers	10
Brother Printers	2
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	1
Router c819	2
Router c2921	2
Router c1841	23
Router c1921	7
Switch c4510r-e	1
Switch c4507r+e	1
Switch c3750G-24	2
Switch c3750G-48	1
Switch c3750-48	13
Switch c3750V2-48	7
Switch c3560G	2
Switch c3560E	3
Switch c3560X	1
Switch c3560	1
Switch c3550-48	17
Switch c3550-24	19
Switch c2960G-24	2
Switch c2960G-48	4
Switch c2960S-24	6
Switch c2960S-48	4
Switch c2960x-24	5
Switch c2960x-48	5
AIR-CT5508-K9	1
LAP1141N	9
LAP1142N	48
AIR-CAP1532E-E-K9	1
AIR-AP1852E-E-K9	35
Mitel Mxe	4
Mitel Cxi	6

Mitel IP Sets	700
Mitel 5310 Conferencing Phones	10
HP Tape Library 8096	1
HPE MSA 2050 (Replacement File SAN)	2
HP MSA 2312i (Portal SAN)	1
Panasonic Toughpads	58
Microsoft Surface Pros	122
Microsoft Surface Books	8
Microsoft Surface Laptop	7
Ubiquiti Nanobeam 5AC Gen 2	2

Miscellaneous	Quantity
Mobile Phones	475
iPhones	10
Smartphones	275
MTPAS Enabled Mobile SIMS	96
MDT Enables Data SIMS	87
iPad	54
USB Encrypted USB devices	190
3G Cards/Dongles	23
Modem	51
Fax	8
Scanners	8
Battery Chargers	142
CD Writers	3
CCTV Monitors	12
CCTV VCR	12
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
Door Access Controller Server	1
Door Access Controllers	15
Door Access Card Printer	1
Door Access Cards	313
Door Access Proximity + Pin Readers	15
Door Access Push to Exit buttons	13
Door Access Break Glass Units	13
Running Call Phones	31

Return to Top.

Appendix B – Key ICT Projects and Activities



Fire Control Road Map

Item	Description	Status
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. A Phase 1, technology refresh of the ICCS was completed in March 2018. Phase 2a & 2b is dependant on the ESN project.
ESN	ESN will replace the communication service delivered by Airwave with a national mobile voice and data service for all three emergency services.	A new Incremental transition plan will initially provide a data capability during 2019, with the intention of delivering a secure voice solution late 2019-2020.
CAD-MIS Project	Replacement of computer hardware and the upgrading of Vision CAD and Vision BOSS applications to deliver an enhanced CAD for 2020.	Due diligence is taking place around the Vision 5 Functional Design Specification and initial costs to upgrade to Vision5 from Vision 3.
MDT2A	Rollout to frontline appliances of the new Mobile Data Terminals with the Airbus mobilisation and risk app.	Airbus ScResponse screen wobble issue is preventing rollout, and final bearer solution is yet to be confirmed.
Station Turnout	Rollout of Multitone equipment to replace existing Station End Turnout PCs to meet the deadlines set by the ESN project at the time of the ITHC.	A two Station POC has been successfully completed and the remaining Multitone equipment is being procured for rollout.
MS Contract Renew	Extension of the Moore Stephens StARS contract for the provision of TRM by three years, expiring on 31.8.2021.	MS was challenged on the options for hosting StARS. Negotiations involving ICT, telent and Procurement resulted in a contract extension with a £14.5k p.a saving.

Business as Usual

Item	Description	Status
Vesty Data Network	To provide a cost-effective radio solution to connect the MFRA Vesty Road buildings to MFRA SHQ network infrastructure.	Commercials, Legal and Health and Safety documentation all complete and, at the time of writing, installation is planned for January 2019
Storage Area Network	Existing SAN reached storage capacity and hardware was end of life.	A new SAN solution has been procured and it is in the process of being racked in the SHQ and TDA server rooms.
Mobile Phones	Rollout of Samsung Xcover 4 and J6 mobiles phones to replace the existing Windows mobile Phones.	50 of each model has been purchased and from 01/12/2018 any new or replacement smart phones will be Samsung.
Mitel Phone Upgrade	Replacement of legacy Mitel IP Telephony solution to replace existing hardware due to it becoming end of life.	Final proposal being finalised with a view to placing an order in December. Implementation will be during Q1 2019
Incidents and Requests	These are the day to day disruptions to the ICT Service outside of Business as Usual ICT Services. e.g. loss of internet, e-mail.	At the time of writing there are no major incidents that are outstanding.
Saughall Massie Station	Commissioning of ICT for the new Saughall Massie Station.	Structural build is underway and data lines have been commissioned.
E-Mail Upgrade	This is a project to upgrade Exchange from 2010 to 2016/19 OR a migration to a hybrid O365 solution in the Cloud.	Options for upgrade are being considered and an autumn 2019 is a potential time to carry out this work.
TDA	Project comprises the refurbishment of the TDA and the refurbishment of Station 19. TDA is home to Secondary Fire Control and Disaster Recovery.	Construction works planned for: Feb 2019 – March 2021. AV budget is in the draft five-Year Capital 2019-2024.
CSU - POD	ICT Commissioning for a Command Support Unit with conference facilities on-board.	Vehicle has been delivered and the ICT requirements are being sought.

Other Highlights

Item	Description	Status
ITHC Roadmap	IT Health check 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.
Toughpads and Surface Pros	Rollout of Toughpads for the SIRAH app and Surface Pros in line with Role Based Resourcing (RBR).	At the time of writing 58 Toughpads and 120 Surface Pros have been procured to be rolled out early 2019.
Windows 10 (W10)	Over and above the Toughpads and Surface Pros is the full rollout of W10 across the organisation.	W10 PC build and user guides are being prepared, with a view to commence rollout April 2019. Note: Windows 7 will be end of life in January 2020.
Extended Wi Fi	Upgrade and expansion of Wi Fi in appliance bays to allow the SIRAH app to update.	Complete.
Office 365	As a requirement to align the ICT infrastructure to future app development activities, a move to using O365 may be required.	O365 is being used by NRAT and ISAR. Discussions are underway in the DevOps Alignment Meetings to determine the Dev ask.

Return to Top.

Appendix C 2019/20 – 2023/2024 ICT Five Year Capital Plan – Draft

ICT - Budget 2018/19 to 2022/23

Type of Capital Expenditure		Total Cost £	2018/19 £	2019/20 £	2020/21 £	2021/22 £	2022/23 £	2023/24 £
IT002 ICT Software								
Software Licences		12,000	2,000	2,000	2,000	2,000	2,000	2,000
New Virtualistation Infrastructure		150,000	75,000					75,000
3 Year Licences Antivirus & Filtering		11,000	11,000					
5 Year Antivirus & Filtering Software		200,000					200,000	
MDT Software Solution Refresh		100,000					100,000	
Microsoft EA Agreement (Servers & Security)		288,000	48,000	48,000	48,000	48,000	48,000	48,000
Microsoft EA Agreement (Windows & Office)		823,000	128,000	139,000	139,000	139,000	139,000	139,000
Microsoft EA Agreement (Application Development)		30,000	5,000	5,000	5,000	5,000	5,000	5,000
Microsoft SQL Upgrade		50,000						50,000
Logpoint Security Information and Event Mgmt (SIEM) Refresh		80,000						80,000
		1,744,000	288,000	194,000	194,000	194,000	494,000	399,000
IT003 ICT Hardware								
Desktops (target 20%)		288,640	66,040	40,100	40,100	40,100	40,100	40,100
Tablets & Docking Stations (target 20%)		480,200	150,200	62,000	62,000	62,000	62,000	62,000
Monitors & Monitor Arms (target 20%)		93,300	23,300	14,000	14,000	14,000	14,000	14,000
Peripherals replacement (target 20%)		19,900	4,900	3,000	3,000	3,000	3,000	3,000
Mobile device replacement (target 20%)		66,200	50,200	3,000	3,000	3,000	3,000	3,000
Replacement Backup Tape Drive		25,000				25,000		
IP TV Asset Refresh		61,800	1,800	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				
		1,261,940	296,440	297,100	242,100	172,100	122,100	132,100
IT005 ICT Servers								
Server/storage replacement (target 20%)		412,800	87,600	65,000	65,000	65,000	65,000	65,000
Server/storage growth		104,300	34,300	14,000	14,000	14,000	14,000	14,000
New SAN Solution								
		518,900	121,900	79,000	79,000	79,000	79,000	79,000
IT018 ICT Network								
Local Area Network replacement (discrete)		7,500	7,500					
Network Switches/Routers replacement		277,300	207,300	70,000				
Network Switches/Router growth		44,300	9,300	7,000	7,000	7,000	7,000	7,000
Network Switches/Router - Additional for JCC/TDA Resilience								
Vesty Road Network Link Refresh		40,000		40,000				
IP Telephony								
Wireless Network		74,600	74,600					
		443,700	298,700	117,000	7,000	7,000	7,000	7,000
IT026 ICT Operational Equipment								
Pagers/Alerters		7,400	7,400					
Station End Kit		66,300	5,300	10,000	10,000	10,000	10,000	10,000
Incident Ground Management System		62,500	2,500	50,000				
MDT Replacement (Not incl. in ESMCP)		195,000			120,000			75,000
		310,200	15,200	60,000	130,000	10,000	10,000	85,000
IT058 New Emergency Services Network (ESN)								
ESN Radios / Infrastructure - Estimate	#	152,000	152,000					
		152,000	152,000					
IT060 ICT Station Change								
Saughall Massie Station End Mobilising Equipment		20,000	20,000					
St Helens Station End Mobilising Equipment		20,000		20,000				
General								
		40,000	20,000	20,000				
SHQ/JCC Major Refurbishment								
IT053 JCC Backup MACC/Secondary Control Resilience								
Other IT Schemes								
IT019 Website Development		42,200	42,200					
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)		133,900	23,900			110,000		
IT030 ICT Projects/Upgrades		27,500	2,500	5,000	5,000	5,000	5,000	5,000
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		8,600	8,600					
IT057 Fleet Management System		4,600	4,600					
IT059 ESMCP Project Control Room Integration		183,100	183,100					
IT061 ESMCP ICT Remedial Works		151,800	151,800					
IT062 Capita Vision 3 Update (CFO/058/17)		950,000		950,000				
FIN001 FMIS/Eproc/Payroll/HR Replacement		325,300	75,300		250,000			
		1,884,000	484,000	982,000	282,000	122,000	12,000	12,000
		6,332,740	1,687,240	1,729,100	914,100	584,100	724,100	714,100
Original Approved Budget		3,930,000	942,800	1,028,100	668,100	588,100	728,100	
Current Programme		6,332,740	1,687,240	1,729,100	914,100	584,100	724,100	714,100
Changes		2,402,740	724,840	701,000	246,000	21,000	(4,000)	714,100

Appendix D – Application Status

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.	Containment	31/03/2019
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.	Containment	31/03/2019
Goldmine (Front Range)	This is a CRM used by Fire Service Direct in the Community Fire Safety Arena	Mainstream	16/06/2019
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	31/08/2021
E-Financials & E-Procurement	Finance, stores and procurement package	Mainstream	31/08/2021
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.	Mainstream	26/02/2020
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	31/12/2019
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	31/08/2021
Org Plus	Used by POD to produce organisational charts using the data exported from Resourcelink.	Mainstream	N/A
File Director	Scans and organises images of paper documents used in POD.	Containment	N/A
Civica Tranman	Vehicle Fleet Management System	Mainstream	23/07/2019

Red Kite	Equipment/asset management system. Hosted since April 2010 and used on stations to ensure operational equipment is checked regularly and appropriately maintained.	Mainstream	31/07/2019
Airbus Hydra	GIS solution which provides risk and hydrant data to the incident ground and organisation.	Mainstream	31/05/2019
Draeger	BA Testing Software	Mainstream	07/12/2019
LearnPro (EFS)	eLearning Management Systems provided by eFireService Ltd	Mainstream	30/04/2019
Auto CAD Architecture (Graitec)	CAD (Computer Aided Design) System	Mainstream	06/01/2020
Wall Chart	Training Resource Planner	Mainstream	01/09/2019
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	29/04/2019
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	31/03/2019
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	31/03/2019
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.	Mainstream (moving to sunset)	30/06/2019
Vision 3 FX BOSS	Management Information: providing senior officers with real time incident information and the organisation with incident history for trend analysis.	Mainstream	31/03/2019
AIRBUS Sc-Response	Data Mobilisation and Operational Risk retrieval. As part of the replacement programme for the existing SEED (BRIGID) system, a number of alternative products including ScResponse are under investigation.	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	31/05/2019
OSHENS	Health & Safety MIS.	Mainstream	31/12/2019
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	28/02/2019
Ximes	Shift pattern modeller	Mainstream	18/10/2019

StARS	TRM staffing system provided by Moore Stephens Consulting and hosted by Bluesource.	Mainstream	31/08/2019
AVCO Anycoms	Middleware which reduces the requirement for manual input and transfers files securely between local authorities.	Mainstream	31/12/2019
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	28/02/2019
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 that will replace, streamline and enhance functionality that is currently delivered through their Intranet Portal capturing business plans, business intelligence, performance management, GIS plotting, project and risk management.	Mainstream	31/07/2019
SharePoint 2013	SharePoint Portal is used to provide the corporate intranet and central repository for MFRS core data.	Mainstream	08/11/2019
MapInfo GIS	MapInfo is a geographical information system used within Strategy and Performance to display and analyse geo-spatial datasets.	Mainstream	30/05/2019
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

Return to Top.