

IT Roadmap 2021-2026 Exec Summary

FEBRUARY 15TH 2021



1 Version Control

<i>Version</i>	<i>Summary</i>	<i>Date</i>	<i>Editor</i>
0.1	First draft	07/01/21	TDG
0.2	Revised to summarise the benefits of roadmap	14/01/21	TDG
1.0	Final internal draft	14/01/21	TDG
1.1	Final draft version for review	28/01/21	TDG
1.2	Addition of costs and benefits after review	15/02/21	TDG

2 Document Approval

<i>Version</i>	<i>Date</i>	<i>Approver</i>
1.2	16/02/21	Fabio Negro

3 Table of Contents

1	Version Control.....	2
2	Document Approval	2
3	Table of Contents	2
4	Introduction.....	3
5	Datacentres, Datacentre Networks & Campus Networks.....	5
6	End User Experience Modernisation.....	8
7	Cyber Protection.....	10
8	Service Improvement	12
9	Roadmap plan.....	14

4 Introduction

The “Shared ICT Service Strategy 2019-2022” was approved in January 2020 and sets out the strategic aims and objectives for the service.

To achieve this strategy, we have proposed a new Target Operating Model for the team structure, roles and posts. This operating model aims to address the strategic objectives below, to better our 10,000+ user community:

- Delivering a Quality Service
- Providing Value for Money
- Forging a lasting partnership

However, alongside the people & process improvements set out in the Target Operating Model, there is also a need to refresh and renew our infrastructure to be stable, scalable, and reliable. To achieve this, we have recognised the need to plan the IT investment roadmap for the next 5 years, which articulates what will be required to deliver this technology.

In addition to the Target Operating Model changes which at time of writing is currently in its final stages of approval, and the IT Strategy approved January 2020, we have also recently developed our Cyber Security Strategy; this is detailed separately.

The roadmap outlines the investment that will be required to meet the future direction of the service described in the aforementioned three pillars.

This document summarises, for the areas listed below, what technology change and investment will be needed, and in which forecasted year, for each partner Council:

- Datacentres, Datacentre Networks & Campus Networks
- End User Experience Modernisation
- Cyber Protection
- Service Improvement

The driving ambition is to provide a suite of common tools for each partner to consume and a standard method of monitoring and managing our datacentres, networks and devices to provide efficiency in operation and security protections.

Whilst this document provides an overarching view of the proposed technology changes over the next five years, a more detailed Business Case will be written for each investment to fully detail the total cost of ownership and benefits case.

A summary of the investment estimate over the 5-year period is included in each section (note: this is overall investment, not per partner), along with an indication of the types of benefits targeted by the investment. These are indicated using the tags below:



Reduction in cost of service



Service experience improvement



Security protection



Service resilience & availability

It should be noted that at this early stage, defining empirical benefit targets for each investment is not possible, and this will be defined as part of the development of business cases. Also, many of the items listed have co-dependencies with other investments in the roadmap to fully maximise the outlined benefit

5 Datacentres, Datacentre Networks & Campus Networks

Delivering a modern, common infrastructure that partners can rely on

“The Shared ICT Service will seek to provide a hybrid approach to our storage and compute technology utilising both on premise and cloud-based technology, we will have the ability to transition to the cloud from our on-premises infrastructure and will seek to provide the most cost-effective mechanism of operating.

We will implement unified communications including collaboration, presence, instant messaging as well as voice over IP telephony direct from the device. We will focus on Office365 as the delivery platform but will offer alternatives based on business need.”

Technology Area	5-Year Capital Investment	Benefit Type	Activity
Backups and Disaster Recovery	£2.45m	  	<p>We are replacing our legacy backup solutions in all three partner Councils with one that can provide a robust and resilient solution which further protects us, and our data, from malicious attack.</p> <p>We will implement an automated recovery solution that can, in the event of a disaster or mass failure of services, restore these in order of priority quickly and efficiently.</p>
Storage and Virtualisation	£1.68m	  	<p>We propose to move incrementally from our physical storage and virtualisation infrastructure to a new hyperconverged infrastructure (HCI). This proposed architecture is also a “one datacentre” solution using Disaster Recovery as a Service (DRaaS) which will further enhance our ability to restore quickly (Recovery Time Objectives or RTO) and to a more complete restoration of service (Recovery Point Objectives or RPO).</p>
Internet Connectivity	£0.12m	 	<p>An upgrade to 10Gbps capacity and bandwidth for our internet connectivity is now in place, which enables us to meet our existing & expected future requirements, including the recently increased demand for remote access.</p>

Data Centre Hosting	£1.34m	 	We will seek to further review and, if financially and operationally opportune, consolidate the number of datacentres that we have in place.
Cloud Migration	Sovereign	  	<p>We are supporting Southwark Council’s current programme and will support other partners’ ambitions to migrate to cloud hosted services when agreed upon.</p> <p>We will skill our teams to effectively manage Cloud environments and implement tools to speed the provisioning of cloud resources and to visualise & control the operational costs of cloud resources.</p>
Cloud and Data Centre Automation and Tools	£0.09m	 	<p>We will implement tools that integrate with both public and private clouds that can automate provisioning of virtual machines, improving both the speed & cost of responding to requests from our Partners.</p> <p>As more services move to cloud, we will have an increasing need to control usage costs in this environment, so we will introduce products that will enhance our capability to manage cost.</p>
Data Centre Operating System refresh	£4.14m	 	We envisage that we will have a continual programme of work to replace our aged Microsoft Windows Server operating systems with their finite support lifetime, so that the environment can be effectively managed, patched and supported.
Remote Access Thin Client Solutions	£0.27m	  	Most remote access is now managed via our Direct Access laptops, which has reduced our previous dependency on Thin Client solutions but not entirely replaced this need for some Council services and teams. We will seek to continue to reduce this dependency and to simplify our remote access solutions, replacing Direct Access, which is no longer being developed by Microsoft, with a solution that provides a seamless user experience.
Data Centre Network	£1.67m	 	The connectivity and access control to, and from, our datacentres is critical to all services provided and we will need to refresh these key elements by the lifecycle end of our current equipment, in 2023-24.

Large and Medium Site networks	£2.99m		<p>Updating the Wi-Fi access to more modern WiFi-6 or Wifi-6e in our large and medium sites will offer faster and more secure Wi-Fi access to our devices. We are due to test several options in 2021-22 with a plan to refresh Wi-Fi in all key office locations.</p> <p>Edge switches provide the wired network connectivity from a device such as a laptop or desktop on a wired network connection in the council offices. Lewisham have recently replaced their edge switches, and we plan to replace these in other partner sites with similar technology.</p>
Smaller Site Networks	£0.48m		<p>The STS network covering the council partners is currently extensive, with Southwark alone having over 100 sites with our network equipment. Both Southwark and Brent small sites are due to be refreshed in the next 2 years and, with Lewisham having recently been renewed, a refresh would be due at the end of the roadmap lifecycle. We will seek to replace this network equipment with a robust, secure and resilient solution based on modern network technologies as outlined in the next section below.</p>
Network Controls	£0.41m		<p>We intend to move our network controls from physical devices that require individual management to modern “Software Defined” solutions that are more cost effective for operation:</p> <ul style="list-style-type: none"> • <i>Software Define Networking (SDN)</i> allows the network to be controlled from a central location by programming the behavior of the network through APIs (application programming interfaces). SDN is focused on Local Area Networks (LAN’s) within a single location and offers the flexibility of management to adapt the network to the needs of the organisation very quickly. • <i>Software Defined Wide Area Networking (SD-WAN)</i> focusses on the links between sites over a large geographical area. SD-WAN is provided by and run by a network vendor rather than internal resources and provides considerable control over how data flows across links and using the optimum route to reach its destination.
Telecoms	£0m		<p>We will need to replace, and have the opportunity, to evaluate the networking technologies that should be used to connect partner Councils’ sites. One option being considered is to use SD-WAN over Internet connections. If SD-WAN is implemented, savings would be realised from the decommissioning of our existing telecoms networks and links. Whilst undertaking this change, we will have the opportunity to consolidate supplier contracts, providing better economies of scale.</p>

6 End User Experience Modernisation

Shared Service Strategy – Building a Solid Platform

“We will offer every member of staff a range of devices which can be chosen based on business need; this will include Laptops, Tablets, Desktops and Smart Phones. Each device will be able to access services from any location and any time utilising key shared infrastructure such as GovWifi and GovRoam.”

Technology Area	5-Year Capital Investment	Benefit Type	Activity
Meeting Rooms	£0.3m		Brent & Southwark Audio Visual (A/V) equipment that provides a more engaging experience for those in the room and attending remotely, which is becoming increasingly common in this era. A similar refresh has also been included in the roadmap for Lewisham’s meeting rooms.
Laptops	£9.02m	   	The next laptop refreshes are not due until towards the end of this technology roadmap period, however plans & costs are included to replace laptops for all three partners’ employees. At that time, we will seek to offer a range of devices to meet the needs of the differing use cases & scenarios, and implement the most cost effective and secure device security protections available.
Mobile Devices	£2.22m	   	We continue to offer the best value iPhones (currently iPhone SE) which provide the best longevity for device and operating system support. We will be adding an appropriate Android phone choice during 21/22. The exact offering for the Android option has yet to be agreed, but both offerings are to be managed through the same Mobile Device Management (MDM) platform, InTune, and we plan to migrate all existing phones to this solution in the near future.

Telephony	Sovereign		Over the next five years we will need to review the telephony needs and potentially replace our existing solutions. As the strategy for telephony has yet to be decided, any change is not depicted in the roadmap currently.
End Point Tools	£0.12m		One of the areas that has the potential to make the end user experience more secure and performant is the provision of class leading end point management tools. The implementation of these tools is included in the roadmap, along with the cost saving for retiring our current solutions.

7 Cyber Protection

Shared Service Strategy – Providing a reliable, quality user experience

“Our Service is only as good as the experience our customers receive; therefore, we will introduce proactive monitoring which will alert us to errors before they become issues for our customers.”

Technology Area	5-Year Capital Investment	Benefit Type	Activity
Security Edge devices	£0.94m	  	<p>Our Load balancers and firewalls will require replacement during this roadmap lifecycle. In addition to managing the data traffic & flow, these provide protection to/for our datacentre and network environments.</p> <p>For further protection, we use “Managed Detection and Response”, which provides a service which protects most of the server estate via an agent on each server. This service has proved invaluable in mitigation of breach attempts. We plan to now implement this technology to all laptops, as the security of the Councils’ data & systems are of paramount importance.</p>
Email & Web Protection	£0m (Opex)	 	<p>One of the major attack vectors continues to be by Email and we will be implementing further protections in 21/22 provided by Proofpoint Fraud defense and Proofpoint mail filtering. Proofpoint has proved itself to be a very capable solution, with extra features being added this year to protect Very Attacked Individuals (VAIs) whereby any suspicious email links will be opened in an isolated session, therefore improving protection.</p> <p>The current web filtering solution is provided by a solution due to be renewed in March 2020 as a 3-year tender with options to extend for years 4 and 5. An appropriate web filtering solution is needed to protect the environment from malicious actors and protect staff and public using both Wi-Fi and library computer from inappropriate content. In addition, Real Time Email risk assessment solutions, which use nudge theory to engage with staff on a regular basis, deliver enhanced security awareness with regards to email threats.</p> <p>With the move of more services to “Software-as-a-service” (SAAS) solutions, standard web filters do not give granular enough filtering and logging of actions which take place. Modern solutions can identify new cloud services, identify the use of shadow IT and access the risk of</p>

			identified services. Data loss prevention policies with encryption and data labeling can be applied.
Privilege Account Management	£0m (Opex)		We will implement Privilege Account Management and Privilege Endpoint Protection to further enhance access security alongside our password management solution used by technical teams who, by necessity, have the greatest access to our IT environment. Privileged users are one of the biggest internal risk and threat actors who breach the perimeter will be looking to exploit privileged accounts first, as it enables them to access and create issues across critical systems. For all other users, Endpoint Privilege Management technologies combine application control and privilege management to ensure that only trusted applications run, and that they run with the lowest possible privilege.
Security Information & Event Management	£0m (Opex)		Security Information & Event Management aggregates event data produced by security devices, network infrastructure, host and endpoint systems, applications, and cloud services. This data is combined with contextual information about users, assets, threats & vulnerabilities to provide real-time analysis of events for security monitoring, historical analysis and support for incident investigation, management & reporting.
Patch Management	£0m (Opex)		With the number of servers that are managed, patch management can be time consuming and costly, so we are in the process of purchasing a solution to patch the server estate using agents that simplify the process of patching the operating systems. This would also be used to patch applications installed on the servers. This will help us maintain high protection of systems & servers and keep downtime and service interruption to a minimum.
Media Management	£0m (Opex)		USB and removable media control is one of the NCSC 10 steps to cyber security. More granular solutions than we currently have will be implemented, such as ensuring the removable media is encrypted before use. Where removable media is allowed more policies will be required to ensure the secure sanitisation of the storage media to prevent data loss.
Security Monitoring & Assurance	£0m (Opex)		Each year we need to assess and test our security for compliance and assurance purposes. Penetrations Test are undertaken by accredited suppliers against internet facing services. With the rate of transformation increasing year on year the number of tests are also increasing. STS propose to tender for this supplier to get the best value. In addition to these assessments and checks, we will expand our current vulnerability management solution across the whole estate to understand all of the assets, vulnerabilities and associated risk profile.

8 Service Improvement

Shared Service Strategy – Providing a reliable, quality user experience

“We will review all of our customer interaction points, our communication methodology and our escalation processes to ensure that we are delivering the best possible service experience.

We will continue seeking improvements to our service by proactively monitoring user experience levels and reviewing and acting upon the data that underpins our service.

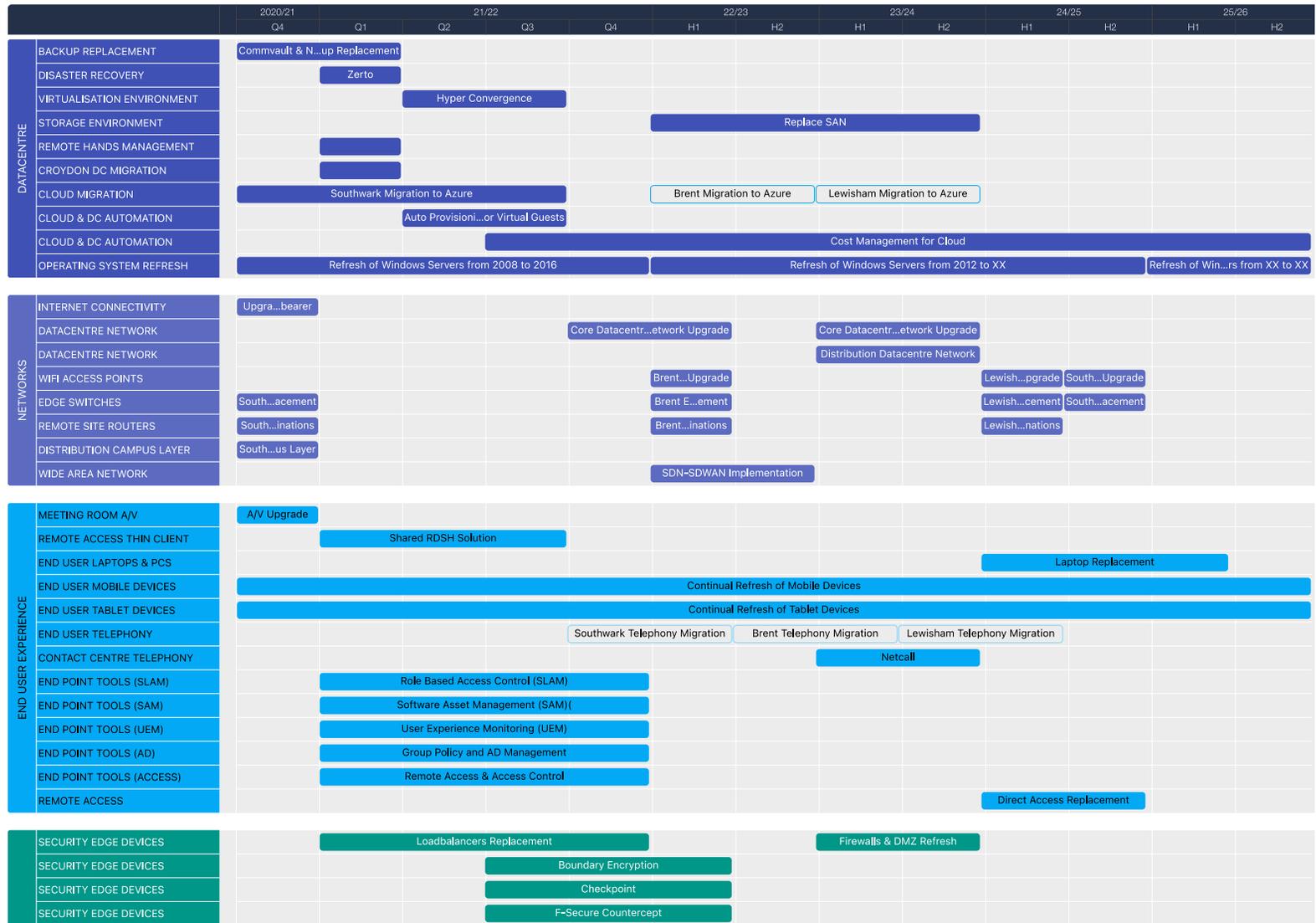
We will ensure that the services that we provide and the mechanism of accessing them are easy to use, intuitive and appropriate for each role.”

Technology Area	5-Year Capital Investment	Benefit Type	Activity
Service Management tooling	£0.33m		Our Service Management system has been the primary user interface now for several years for logging incidents and requests to the shared service. We are due to review the needs of our entire operation (including project management, asset management & supplier management) and, if beneficial, replace this solution within the roadmap period.
Configuration Management	£0.18m		The shared service has invested considerable time and resources in improving the monitoring and alerting of its infrastructure: both hardware and services. The primary tools used are Microsoft System Center Operations Manager (SCOM), Microsoft Azure Resource Monitoring, Solarwinds Network Performance Monitor (NPM). We are due to review the needs of our entire operation and, if beneficial, replace these solutions within the roadmap period.
Business Automation agents	£0.05m		Solutions such as virtual chat agents, Robotic Process Automation (RPA), WhatsApp for Business & iMessage for Business may well be utilised in all three partner councils in future, and we will seek to use these solutions within the service for the benefit of our user community where this is beneficial. Some RPA is already in place in Brent.

IT Service Messaging	£0.08m		<p>Having the ability to communicate to staff effectively in the event of an outage would improve our handling of such outages and there are solutions available to proactively alert staff affected by a particular outage, which we plan to implement over the period.</p>
Asset Management Tools	£0.14m		<p>Our current asset management tools and processes are too disaggregated to enable cradle-to-grave asset management of our & devices estate. The intent is that we manage our entire estate via one solution, which will provide benefits for maximising our asset life & utilisation (e.g. reallocation of assets rather than purchase).</p>
Staff technical training	£0.08m		<p>The shared service is committed to providing the necessary technical training to staff to enable them to carry out their tasks to the best of their abilities. We will invest a part of our training budget with a training provider, as this will bring significant discounts on retail prices across the available curriculum. In addition, we will fund the cost of certification exams where appropriate as these will benefit the shared service in being able to show our expertise and knowledge in key product areas.</p>

9 Roadmap plan

A full view on one page can be found [here](#), however below us the full roadmap of all activities mentioned in this document.



		2020/21			21/22			22/23		23/24		24/25		25/26	
		Q4	Q1	Q2	Q3	Q4	H1	H2	H1	H2	H1	H2	H1	H2	
CYBER PROTECTION	SECURITY EDGE DEVICES				Manage Detection Response										
	CONTENT FILTERING					Email Filtering									
	CONTENT FILTERING						Proofpoint Fraud Defence								
	CONTENT FILTERING						Proofpoint Filtering								
	CONTENT FILTERING						Web Filtering								
	CONTENT FILTERING						Forcepoint								
	CONTENT FILTERING						Real-time Email Risk Assessment								
	ACCESS MANAGEMENT						Cloud Access Security Broker								
	ACCESS MANAGEMENT						Password Safe								
	ACCESS MANAGEMENT						Privilege Account Management								
	ACCESS MANAGEMENT						Privilege Endpoint Protection								
	ACCESS MANAGEMENT						USB Lockdown Tools								
	MANAGEMENT & ASSESSMENT							Security Information and Event Management							
	MANAGEMENT & ASSESSMENT							Security Assessments & Penetration Tests							
	MANAGEMENT & ASSESSMENT							Vulnerability Scanning and Management							
	MANAGEMENT & ASSESSMENT							Operational Centre Investment (Mission Control)							
	MANAGEMENT & ASSESSMENT							Service Operations Centre Setup							
	MANAGEMENT & ASSESSMENT							Distributed Denial of Service (DDOS) Protection							
	MANAGEMENT & ASSESSMENT							Patch Management Tooling							
	MANAGEMENT & ASSESSMENT							Cyber Insurance							
SERVICE IMPROVEMENT	CONFIGURATION MANAGEMENT				CMDB Tooling				Configuration...nt Implementation						
	DEVICE & ASSET MANAGEMENT				Asset Management Tooling										
	SERVICE MANAGEMENT								Service Manag...Tooling Regresh						
	OPERATIONAL MONITORING								Operational Ma...ent Dashboards						
	BUSINESS AUTOMATION							Robotic Process Automation							
	USER SURVEYS						Feedb...uttons								
	IT HUB						IT Hub...ueuing								
	SKILLS TRAINING						Continual Technical Training for Staff								



February 2021

Created by:

Tim Green – Senior Programme Manager

Jason Carney – Enterprise Architect

Kevin Ginn – Head of Operations