Appendix 1
Brent IT Roadmap

Technology Roadmap 2021-2025 Exec Summary

MARCH 31ST 2021

Brent

Version Control

Version	*Summary*	*Date*	*Editor*
1.0	First issue	26/03/21	TDG
1.1	Amended after review	29/03/21	TDG
1.2	Amended to include cost breakdown	31/03/21	TDG

Document Approval

Version	*Date*	*Approver*
1.2	31/03/21	Fabio Negro
	31/03/21	Sally Chin

Table of **Contents**

Introduction

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

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

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

The total Capital Spend for FY2021/22 to FY2024/25 is forecast to be £10.3m.

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, 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.

Overall, during this 2021-2025 period, we will annually review our Service Levels and Key Performance Indicators. With the investment & changes listed within this roadmap, we aim to improve our availability KPI from the current 99%, to 99.9% and we will seek to improve on other SLAs and KPIs as we progress.

Datacentres, Datacentre Networks & Campus Networks

Total Investment £5m			
Technology Area	**Capital Investment**	**Benefit Type**	**Activity**
Backups and Disaster Recovery	21/22 £850k		We are replacing our legacy backup solutions for the Council with one that can provide a robust and resilient solution which further protects us, and our data, from malicious attack. 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.
Storage and Virtualisation	21/22 £100k 22/23 £250k 23/24 £100k 24/25 £100k		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).
Internet Connectivity	21/22 £50k		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.
Data Centre Hosting	21/22 £50k 22/23 £500k		We will seek to further review and, if financially and operationally opportune, consolidate the number of datacentres that we have in place.
Cloud and Data Centre Automation and Tools	21/22 £50k		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. 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.

Data Centre Operating System refresh	£300k per year (Total £1.5m)		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	21/22 100k		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	23/24 £300k		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	21/22 £500k 22/23 £200k		Updating the Wi-Fi access to more modern WiFi-6 or Wifi-6e in 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. 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.
Smaller Site Networks	22/23 £200k		Network equipment at smaller Brent sites are due to be refreshed in the next 2 years. 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.
Network Controls	23/24 £200k		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: • *Software Define Networking (SDN)* 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. • *Software Defined Wide Area Networking (SD-WAN)* 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	Reduction in revenue costs with SD-WAN		We will need to replace, and have the opportunity, to evaluate the networking technologies that should be used to connect Council 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.

End User Experience Modernisation

Total Investment £3.7m			
Technology Area	**Capital Investment**	**Benefit Type**	**Activity**
Meeting Rooms	21/22 £120k		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.
Laptops	24/25 £2.9m		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 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	£150k per year (Total £600k)		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 as an alternative. 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	22/23 £30k		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	21/22 £40k		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.

Cyber Protection

Total Investment £1.1m			
Technology Area	**Capital Investment**	**Benefit Type**	**Activity**
Security Edge devices	21/22 £250k		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. 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 Council’s data & systems are of paramount importance.
Email & Web Protection	N/A		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. 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. 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 identified services. Data loss prevention policies with encryption and data labeling can be applied.

Privilege Account Management	N/A		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	22/23 £600k		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	21/22 £50k		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	21/22 £50k		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	21/22 £50k 24/25 £60k		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.

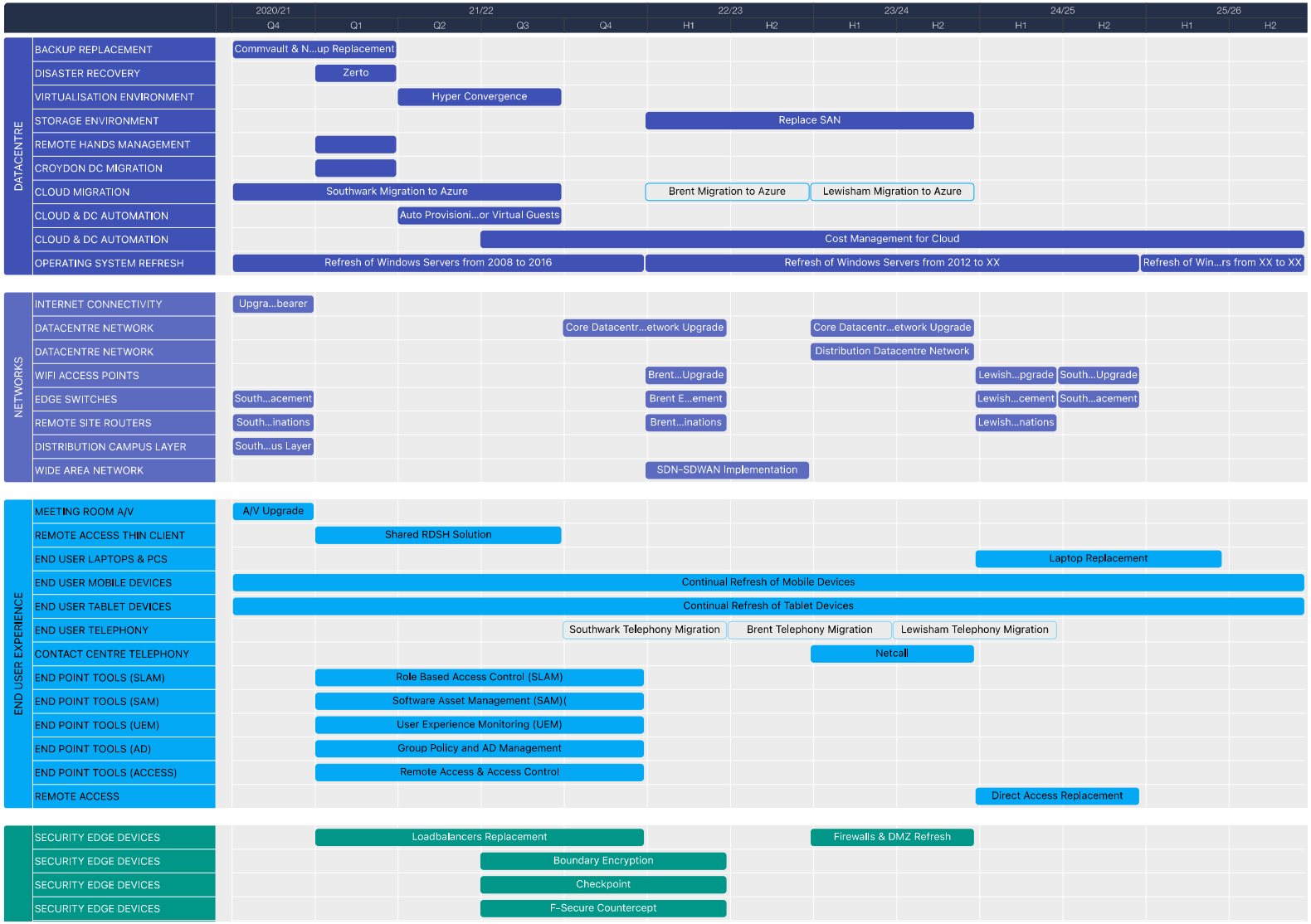
Service Improvement

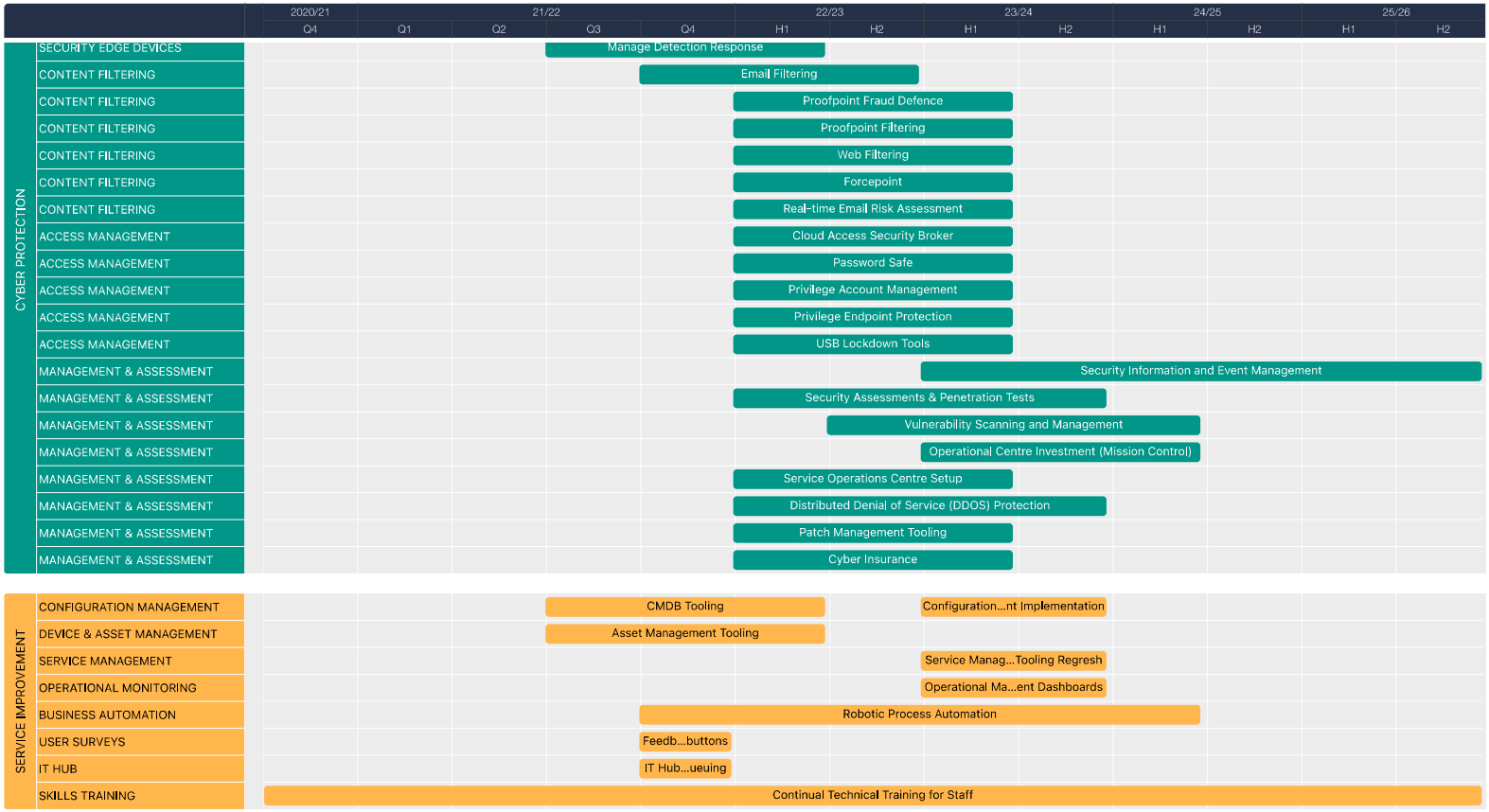
Total Investment £0.5m			
Technology Area	**Capital Investment**	**Benefit Type**	**Activity**
Service Management tooling	23/24 £200k		Our Service Management system has been the primary user interface now for several years for logging incidents and requests. We are due to review the needs of our entire operation (including project management, asset management & supplier management) and, if beneficial, replace this solution within the roadmap period.
Configuration Management	23/24 £100k		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	22/23 £50k		Solutions such as virtual chat agents, Robotic Process Automation (RPA), WhatsApp for Business & iMessage for Business may well be utilised 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	21/22 £50k		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.
Asset Management Tools	21/22 £50k		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 & utlilisation (e.g. reallocation of assets rather than purchase).

Staff technical training	N/A		We are 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 IT service in being able to show our expertise and knowledge in key product areas.

Roadmap plan

Below is 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...buttons
IT HUB
IT Hub...ueuing
SKILLS TRAINING
Continual Technical Training for Staff

March 2021

Created by:

Tim Green – Senior Programme Manager

Jason Carney – Enterprise Architect

Kevin Ginn – Head of Operations