

Joint IT Committee (Brent, Lewisham and Southwark)

Tuesday 2 March 2021

6.30 pm

This will be held as a virtual meeting.

For further information please visit:

<https://www.brent.gov.uk/your-council/democracy-in-brent/local-democracy/live-streaming/>

Membership

Councillor Kevin Bonavia
Councillor Amanda De Ryk
Councillor Rebecca Lury
Councillor Alice Macdonald
Councillor Margaret McLennan
Councillor Tom Stephens

Reserves

Councillor Stephanie Cryan
Councillor Brenda Dacres
Councillor Neil Nerva
Councillor Catherine Rose
Councillor Krupa Sheth
Councillor Jonathan Slater

INFORMATION FOR MEMBERS OF THE PUBLIC

Access to information

You have the right to request to inspect copies of minutes and reports on this agenda as well as the background documents used in the preparation of these reports.

Babysitting/Carers allowances

If you are a resident of the borough and have paid someone to look after your children, an elderly dependant or a dependant with disabilities so that you could attend this meeting, you may claim an allowance from the council. Please collect a claim form at the meeting.

Access

The council is committed to making its meetings accessible. Further details on building access, translation, provision of signers etc for this meeting are on the council's web site: www.southwark.gov.uk or please contact the person below.

Contact Tim Murtagh via email: tim.murtagh@southwark.gov.uk



Joint IT Committee (Brent, Lewisham and Southwark)

Tuesday 2 March 2021

6.30 pm

This will be held as a virtual meeting.

For further information please visit:

<https://www.brent.gov.uk/your-council/democracy-in-brent/local-democracy/live-streaming/>

Order of Business

Item No.	Title	Page No.
1.	JOINT IT COMMITTEE AGENDA PACK 2 MARCH 2021	1 - 65
	This will be a virtual meeting. For further details please visit – https://www.brent.gov.uk/your-council/democracy-in-brent/local-democracy/live-streaming/	

Date: 1 March 2021

Joint Committee of the London Boroughs of Brent, Lewisham and Southwark

Tuesday 2 March 2021 at 6.00 pm

This will be held as a virtual meeting.

The link to view the meeting is available by clicking [HERE](#)

Membership:

Members:

Councillor Margaret McLennan (London Borough of Brent)
Councillor Tom Stephens (London Borough of Brent)
Councillor Kevin Bonavia (London Borough of Lewisham)
Councillor Amanda De Ryk (London Borough of Lewisham)
Councillor Rebecca Lury (London Borough of Southwark)
Councillor Alice Macdonald (London Borough of Southwark)

Substitute Members:


Councillor Neil Nerva (London Borough of Brent)
Councillor Krupa Sheth (London Borough of Brent)
Councillor Brenda Dacres (London Borough of Lewisham)
Councillor Jonathan Slater (London Borough of Lewisham)
Councillor Stephanie Cryan (London Borough of Southwark)
Councillor Catherine Rose (London Borough of Southwark)

For further information contact: Rashella Rapley, Governance Officer
0208 937 3051 - rashella.rapley@brent.gov.uk

For electronic copies of minutes, reports and agendas, and to be alerted when the minutes of this meeting have been published visit: democracy.brent.gov.uk

The press and public are welcome to attend this meeting. The link to view the meeting is available [HERE](#)



	Joint Committee of the London Boroughs of Brent, Lewisham and Southwark 2 March 2021
	Report from the Managing Director of Shared Technology Service
Shared Technology Services Update	

Wards Affected:	N/A
Key or Non-Key Decision:	N/A
Open or Part/Fully Exempt: <small>(If exempt, please highlight relevant paragraph of Part 1, Schedule 12A of 1972 Local Government Act)</small>	N/A
No. of Appendices:	Four Appendix A: Shared Technology Services Performance Pack Appendix B: Cloud Programme Update Appendix C: Shared Technology Technical Roadmap Executive version Appendix D: Shared Technology Services Cyber Strategy
Background Papers:	None
Contact Officer(s): <small>(Name, Title, Contact Details)</small>	Fabio Negro Managing Director of Shared ICT Services Fabio.Negro@brent.gov.uk

1. Purpose of the Report

- 1.1 This report provides an update on Shared Technology Services (STS).

2. Recommendation(s)

- 2.1 The STS Joint Committee is asked to:
- Note the actions being taken in Section 3 – Detail
 - Note the contents of the Performance Pack as attached in Appendix A

3. Detail

Summary

- 3.1 During the four-month period, October and November saw similar call volumes of just over 8,000 calls each month in STS queues. As expected, call volumes dropped in December to 6,393 due to the Christmas break and this allowed us to reduce open call numbers. In January call numbers have risen back to pre-Christmas levels.
- 3.2 A Shared Technology Service Cyber Strategy was created to outline our approach in defending the residents and council data. The Strategy has been included in Appendix D.
- 3.3 In the last quarter, good progress has been made with the Continuous Service Improvement Plan activities and a further 10 activities are now closed down.
- 3.4 The production of the Technology Roadmap has been produced please see Appendix C for further detail.
- 3.5 As a result of centralising the management of audits it has highlighted how many STS have been managing which total 15 Audits, which compromises of:
 - 7 reports that have final reports and recommendations and are being tracked. STS have completed most of the management actions see table below for more detail
 - 2 legacy audits from 2018/19 for Lewisham and Southwark and all management actions have been completed
 - 6 audits for 20/21 that are in varying stages between scoping and receiving final reports with recommendations and management actions.
- 3.6 The Target Operating Model was approved by Joint Committee on 18th January.
- 3.7 We are now in a 30-day period of consultation with the staff members on the proposed restructure, which was initiated on Monday 8th February.
- 3.8 The Shared Technology Service (STS) is forecasting an underspend of £2,418 for 2020-21, against a total budget of £14,477,314. The underspend is primarily due to investment cases covering identified revenue pressures.

Service Performance

- 3.9 The shared service logged 45,407 tickets between 1st October 2020 and 31st January 2021 (an average of 11,350 tickets per month) against 36,658 in last period, July to September 2020 (an average of 12,220 tickets per month), these tickets consisted of both issues and service requests.

This is broken down by (previous period numbers in parentheses):

- Shared ICT Services – 28,982 - an average 7,245 per month (24,780 - an average of 8,260 per month)
 - Brent Applications Teams – 8,562 - an average of 2,140 per month (6,695 - an average of 2,231 per month)
 - Lewisham Applications Teams – 3,687 - an average of 921 per month - (2,854 - an average of 951 per month)
 - Southwark Application Teams – 1,452 - an average of 363 per month (1,426 - an average of 475 per month)
 - Other customers (e.g. LGA) – 2,724 - an average of 681 per month (903 - an average of 301 per month)
- 3.10 Since the Joint Committee last met (4 months), there have been 14 priority 1 incidents within STS queues, of which 7 were resolved within the service level agreement. There were also 3 non-STS related P1s. This is an increase over the previous period and more detail can be seen in the performance pack – but 7 of the calls were related to the public web sites of Lewisham and Southwark councils. There were three main infrastructure-related failures, but these centred around ageing components that will be due for decommission, replacement or upgrade in the coming year. The shared service continues to focus on infrastructure and process improvements in this area to reduce these numbers.
- 3.11 During the four-month period, October and November saw similar call volumes of just over 8,000 calls each month in STS queues. As expected, call volumes dropped in December to 6,393 due to the Christmas break and this allowed us to reduce open call numbers. In January call numbers have risen back to pre-Christmas levels.
- 3.12 The number of priority 1 incidents increased in this reporting period, mainly due to multiple issues with the public web sites of Lewisham and Southwark councils. There were three main infrastructure-related failures but centred around ageing components that will be due for decommission, replacement or upgrade in the coming year.
- 3.13 Priority 2 and 3 issues within STS queues have seen an average of 72% and 71% compliance with the service level agreements (against 57% and 64% reported for the previous period). STS has placed considerable emphasis on improved call management and that can be seen in the improved SLA performance. STS will continue to work to improve the service levels.
- 3.14 The Joint Committee had requested further detail as to the categorisation of the P2 and P3 calls. The development of additional monitoring tools in PowerBI has allowed us to identify areas of focus.
- 3.15 The top six categories for P2 calls (69) logged in STS Hornbill queues during October to January are as follows:

Category	Number of Calls
Server Issues	20
Software/Firmware	8
Network Issues	5
Application database	5
Telephony	4
Service password issues	2

- 3.16 The top six categories for P3 calls (only the first 10,000 can be analysed in Hornbill, but total was 10,316) logged in STS Hornbill queues during October to January are as follows:

Category	Number of Calls
Advice/Training given	2453
Software/Firmware	1007
Folder/File issues	506
Password Reset	391
Hardware	357
Restart/reboot	151

- 3.17 Priority 4 service requests within SICTS queues for this reporting period have an 80% compliance with the service level agreements (compared with 78% for the previous reporting period).
- 3.18 The shared service operated a programme (Call Biltz) to reduce the number of open/on-hold tickets within Hornbill. At the height of the first Covid-19 wave, the shared services open/on-hold queue had over 4,500 tickets, but over the Christmas period we were able to reach the target of 1,500. Since then, due to demand in January, the count now stands at approximately 2,400 but this is still a considerable reduction on the original total. With the STS restructure imminent, we expect to be able to reduce numbers further. The impact of this, and of improved call handling and management processes that have been instigated, has led to improved SLA performance.
- 3.19 Net Promoter score is an industry standard for monitoring the experience of our service. Anything above zero is considered to be good, with above 50% ranked as excellent. In this reporting period we have been able to achieve over 60% - this is detailed in the accompanying performance pack.
- 3.20 Hornbill, our customer portal, is being developed to present a more user-centric experience which should lead to better categorisation of calls being logged. This in turn should allow us to introduce more automated workflows to speed allocation and resolution of incidents and request tickets. A trial of the new experience has been taking place in the partners with positive feedback.
- 3.21 Due to the much greater requirement for remote/home working and to support the new backup system (which uses cloud-based storage), the Internet link bandwidth in the STS datacentres is being upgraded from 1Gb to 10Gb. The

STS Croydon datacentre link was upgraded in January with the STS Brent datacentre link to be upgraded in March. This will also mean that we have enough bandwidth to cope with all connections should one of the links fail. It will also allow us to consolidate Southwark Council's Internet links when the existing contract for those circuits ends in 2022.

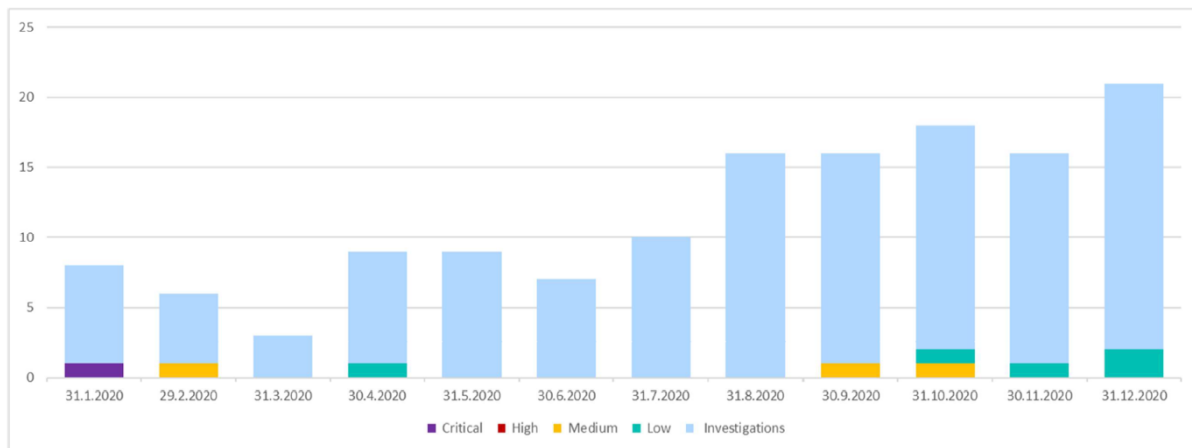
- 3.22 The telephone support line which was introduced at the start of the Covid-19 situation has been maintained and while popular, the engineer resource requirement for this has placed a pressure on the service desk, and response times have increased.
- 3.23 The out of hours support telephone service (introduced in March 2020), is backed up by a third-party and has proved successful. As part of the restructure and new target operating model, it is intended to extend that service to 24x7x365 through a third-party, to provide a more responsive telephone service for urgent/time-sensitive support calls where the Hornbill Portal may not provide the timeliest resolution – this will take the place of the in-hours telephone service currently provided (please see previous point). This service will add additional capacity to the telephone lines (and there will be an agreed SLA answer time for any telephone calls into the service desk) plus this will free up engineer resources on the service desk to attend to other calls.

It is anticipated this service will be operational by April 1st 2021. STS will operate an out of hours P1 escalation service to manage any major incidents that may occur outside of core hours.

Cyber Security

- 3.24 During this last period, we have not had any serious cyber security issues, we continue to work with a third party recommended by the National Cyber Security Centre to proactively monitor our environment.
- 3.25 As we continue to harden our infrastructure, we see a continuing reduction in security incidents over the past 12 months. Other than false positives, no incidents have been raised in this period by our threat protection partner.

Initial investigations take place when anomalies are spotted such as vulnerability scans or out of the ordinary AD Sync actions. In some cases, these are closed before contacting shared service in others we may be asked to confirm that an action is known about and expected. Both the logs show here related to advice about the SolarWinds supply chain attack. The full report from F-secure can be made available.



3.26 The internal infrastructure was critically behind on some of our security controls and there has been an active programme to bring the infrastructure to acceptable levels. During the coming months there will be a continued focus on the hardening of our infrastructure. Tools have been purchased to aid both vulnerability management and patching across the server estate, to be deployed by end of March 2021.

3.27 Much work has taken place both with MHCLG and the LGA in response to several high-profile cyber-attacks. Responding to surveys covering the following areas of cyber security.

- Identify
- Protect
- Detect
- Respond
- Recover

Initial focus for the shared service has been on the respond and recover given the importance of offline backups in the case of a ransomware incident.

A decision was taken to bring forward the procurement and installation of a new backup system to ensure the security and integrity of the backup data as well as enhanced recovery capability in the event of an attack such as Ransomware. A Rubrik backup solution has been procured and it is expected to be fully installed and configured by the end of March this year. This will give us both short term (14 days) on-premises backup storage (in the form of a backup appliance that has an immutable file system and multi-person/multi-factor authentication for any administrative action that could modify or delete backed-up data) and Azure cloud storage (replicated between multiple Azure datacentres) for longer term (13 months) backup storage. This configuration complies with NCSC guidelines for a secure backup solution. Work is ongoing with MHCLG to obtain funding for projects related to the ongoing ransomware remediation effort

3.28 Public Service Network (PSN) compliance allows the councils to connect to other government networks such as the NHS and DWP. Brent is currently compliant,

Lewisham has resubmitted with updates in February and Southwark have had a health check and a submission is being prepared.

- 3.29 Payment Card Industry (PCI) is the accreditation required to allow organisations to take electronic payments such as those we have on the website and in Libraries. This only applies if the council manage the payment service. Brent and Lewisham are both currently accredited. Southwark outsource its payment service therefore not applicable.
- 3.30 Brent and Lewisham have an old smartphone estate which is being scheduled for upgrade. These devices are falling below current security compliance levels. Brent have started a replacement programme and are near to completion. Lewisham are considering its model around mobile telephony and strategy is currently being developed. Southwark have very few outstanding devices and are being managed on a case-by-case basis.
- 3.31 A considerable amount of work has gone into managing numbers of accounts across the three councils. A review of the starters, movers and leavers process has been completed to ensure that we have as few enabled accounts as possible. This limits the possibility of them being exploited and is also important due to licencing and the costs surrounding that.
- 3.32 We have seen 15.3 million emails attempt to reach the councils within a 30-day period. Over 85% of these emails were stopped because they were spam or malicious email such as ransomware. The layers of protection have ensured that the councils have avoided serious incidents.
- 3.33 A Shared Technology Service Cyber Strategy was created to outline our approach in defending the residents and council data. The Strategy has been included in Appendix D.

Continuous Service Improvement Plan

- 3.34 In the last quarter, good progress has been made with the activities and a further 10 activities are now closed down.
- 3.35 To continue with this good progress, the STS Senior Leadership Team have been reviewing progress of the CSIP every month, and quarterly reviews are scheduled with the Operational Management Group.
- 3.36 There have been no tasks added to the plan in the last quarter and there are 16 tasks remaining on the plan, 10 of which are in progress and the remainder scheduled to commence after implementation of the new Target Operating Model organisational structure, when dedicated resources for Service Design and Improvement are expected to take ownership of the plan and any additional items.
- 3.37 This team will be tasked with identifying and prioritising further service improvement opportunities such as continuous improvement to our portal, development of a detailed Service Catalogue, and improving our overall processes, data quality & reporting.
- 3.38 The current plan to improve our service is based on the categories below:

- Strategy & Governance
- Network & Communications
- Infrastructure
- Finance & Procurement
- Enterprise Support
- Customer Experience
- Service Desk

3.39 The launch of a redesigned portal, originally planned for Q4 2020, has been deferred until late Q1 2021 after assessing after assessing some operational issues. When launched, we expect this portal to improve the categorisation of user reported issues as well as the subsequent handling and reporting; the ultimate aim being to reduce the average time to resolution.

Audits

3.40 Since the last Joint Committee in October 2020 all audits are now managed centrally by the Head of Service and are reviewed monthly by STS senior leadership team to ensure that recommendations and management actions are tracked through to completion.

3.41 As a result of centralising the management of audits it has highlighted how many STS have been managing which total 15 Audits, which compromises of:

- 7 reports that have final reports and recommendations and are being tracked. STS have completed most of the management actions see table below for more detail
- 2 legacy audits from 2018/19 for Lewisham and Southwark and all management actions have been completed
- 6 audits for 20/21 that are in varying stages between scoping and receiving final reports with recommendations and management actions:
 - Brent – **IT Asset Management Review**
 - Brent – **IT Project Review**
 - Lewisham - **Smart tech roll out project**
 - Lewisham - **Cyber – Remote working arrangements**
 - Southwark – **Mobile phone management**
 - Southwark – **Asset Management**

3.42 STS have met with the borough IT Directors and audit departments and are working collaboratively to agree 21/22 audits plans. Plans will be shared at the next Joint Committee once they have been agreed.

Brent	-	IT	Sourcing	Audit
This audit is to assess the design and operating effectiveness of the IT sourcing.				
Create third Party Data Register			Medium	Completed

Service Level Agreement (SLA) Strategy and Performance Monitoring (Contract Monitoring)	Medium	Completed
Business Continuity Management (BCM) and Disaster Recovery (DR)	Medium	Completed
Third Party Risk Management Framework / IT Procurement Policy	Medium	Completed
Central Repository & Register for Contracts	Low	Completed

Brent - IT Governance Audit

This audit is to ensure that appropriate financial, decision-making and portfolio management structures are in place so that IT can enable the Council to deliver on its objectives and mandate.

Introduction of SLA Penalties	Medium	Completed
Creating a single risk register for the SICTS	Medium	Completed
EOS (end of support) and EOL (end of life) IT Infrastructure	Medium	Completed
Introduction of IT Organisational Chart	Low	Completed

Brent - IT Platform Governance review

This audit is to ensure that IT platforms (Microsoft Windows) have appropriate governance, operational and security controls and that the security configurations are maintained and kept updated.

Authorised staff members can make changes	High	Completed
Monitoring of user activity	High	Completed
User access review	Medium	Completed
Platform Policies / Standard Operating Procedures	Medium	Completed
Unsupported Operating Systems	Low	Completed

Brent - IT Disaster Recovery

The objective of this review is to evaluate the design of the Shared Service's IT DR planning framework and processes to assess whether they are appropriate, complete and robust, and to explore whether there is sufficient assurance that the arrangements will operate in practice.

Failure to periodically test the IT DR plan can result in the systems not being recovered within required recovery time objectives should the need for DR be invoked.	High	In progress
If the ITDR capability is not overseen by an appropriate organisational structure representing all business services at an effective level, there is a risk that it will not meet business recovery requirements.	Medium	In progress
Failure to ensure that the DR plan is updated regularly especially after significant changes in the business or ICT environments can result in misalignment between achievable recovery times of key systems, not meeting	Medium	In progress

the objectives and expectations of the Council to deliver its services.		
If the criticality of systems is not established and reviewed on a regular basis, or as soon as the system is implemented, and taking account of all Council business systems, it may mean the correct level of risk is not associated with it failing and impact the priority of recovery action taken in the event of disaster.	Medium	In progress
The recovery of the applications and services in scope may be delayed if supporting interfaces and dependent systems are not defined and the recovery tested simultaneously. This could result in failure to deliver critical services within the agreed timeframes.	Medium	In progress
Lack of established and defined procurement third party risk assessment processes may lead to business disruption at the supplier not being effectively flagged and resolved. This may have an adverse impact on Council operations.	Medium	In progress
If an incident is replicated at both sites this effectively removes any option to failover to a known safe state and environment. The only option remaining would be to rebuild and restore services from a network-isolated backup copy. If restoration is not pre-planned, and the restoration time known, the resulting business impact is likely to be adverse.	Medium	In progress
Staff may receive insufficient training or may not be made aware of IT DR arrangements and their role within them, which may result in an ineffective response.	Medium	In progress

Lewisham - Telecommunications Audit

This audit focuses on resilience, system security, application governance of the telephony system.

System Security – Administrator Access	Medium	Completed
System Security – Monitoring of Unsuccessful Logins	Medium	Completed
System Security – Generic Phone Handset and Voicemail Passwords	Medium	Completed
System Security – Generic Phone Handset and Voicemail Passwords	Medium	Completed
Disaster Recovery and Maintenance – Disaster Recovery Arrangement	Medium	Completed
Resilience, Disaster Recovery and Maintenance – 3rd Party Assurance over the 8x8 Network	Medium	Completed
Application Management and Governance – Telephony Asset Management	Low	Completed
Application Management and Governance – User Management	Low	Completed
System Security – Monitoring of Remote Access Ports	Low	Completed
System Security – Security Policy	Low	Completed

System Security – Automated Switchboard Maintenance	Low	Completed
System Security – Reverse Charge Calls	Low	Completed
Call Restrictions – Call Barring and Restrictions	Low	Completed
Resilience, Disaster Recovery and Maintenance – Switch Configuration Backups	Low	Completed
System Monitoring Reports and Value for Money (VFM) – Call Logging	Low	Completed
System Monitoring Reports and Value for Money (VFM) – Telephone Bill Reconciliation	Low	Completed

Southwark - Website Security and Maintenance This audit appraised the design and operational effectiveness of the Council's procedures for identifying and protecting its website and for managing the security and maintenance risks on an ongoing basis.		
Resilience and continuity arrangements for web application may not be adequate to ensure timely recovery following an attack	High	Completed
Patch management, change control and antivirus for the website is ineffective and lead to outdated services, unauthorised changes and unprotected servers	Medium	Completed
Resilience and continuity arrangements for web applications may not be adequate to ensure timely recovery following an attack	Medium	Completed
Vulnerability scanning and remediation of web servers and applications is ineffective and leads to critical vulnerabilities not being resolved	Medium	Completed
Patch management, change control and antivirus for the website is ineffective and lead to outdated services, unauthorised changes and unprotected servers	Low	Completed
Policies and procedures for website maintenance and administration may not be up to date, or understood and followed by administrators	Low	Completed
Patch management, change control and antivirus for the website is ineffective and lead to outdated services, unauthorised changes and unprotected servers	Low	Completed

Southwark - Shared ICT Review This Audit focuses on governance and performance issue resolution and future planning.		
As a result, there is a risk that the resolution of the major incidents are not within the SLA target. Furthermore, there is a risk of any tasks assigned in a meeting may not address the root cause of the issues discussed and that trends may not be identified for categorisation of the issues.	Medium	Completed

As a result, there is a risk that the IAA may not provide the councils with the updated level of service they require	Low	Completed
---	-----	-----------

Where audits have all actions complete, they will be removed from future Joint Committee reports.

Road Map

- 3.43 The production of the technology roadmap has been produced please see Appendix C for further detail.
- 3.44 The technology road map is now being enacted and we have added estimated timescales for Business Cases to be written and approved, so that we are able to keep to planned spend each year.
- 3.45 For the identified 5 technology themes, the top-level capital investment projections for 5 years are as follows:
1. Data Centre Improvements: £11m
 2. Campus Networking Refresh: £4m
 3. End User Experience Modernisation: £12m
 4. Cyber Protection: £4m
 5. Service Improvement: £1m
- 3.46 The IT roadmap will be integral for the design of the future target operating model and has been developed in tandem with this. For example, the roadmap highlights the potential need for several project resources to deliver the technology changes.
- 3.47 A draft Executive Summary of the key elements in the roadmap has now been written and distributed for comment.

Target Operating Model

- 3.48 The Target Operating Model was approved by Joint Committee on 18th January.
- 3.49 We are now in a 30-day period of consultation with the staff members on the proposed restructure, which was initiated on Monday 8th February.
- 3.50 After consultation has been completed, the team structure will be finalised, and all vacancies will be advertised internally to the team initially.
- 3.51 Following this internal recruitment round, remaining vacancies will then be advertised to partner councils and externally. We have initiated four workstreams to progress with this recruitment:
1. Talent Acquisition – Executive search, digital marketing across multiple channels, LinkedIn recruitment.
 2. Internal Process – Selection & interview process, internal communications and reporting.
 3. Up skilling – Training needs analysis for new placements.

4. Engagement – Defining candidate journey & onboarding in the current remote working environment.
- 3.52 Our target implementation date for the new structure is 10th May 2021, subject to successful recruitment, selection and onboarding of new colleagues.

Lewisham Homes

- 3.53 STS and Lewisham Council have produced a report for the provision of IT infrastructure support services for Lewisham Homes that was taken to and approved by the Joint Management Board.
- 3.54 The report recommended that the current model of apportionment will continue, and LH will be added to the Lewisham council contribution to the shared service. Governance will continue as it operates with the same membership. Lewisham Homes will be represented by Lewisham council. Lewisham Council will present its proposal (based on the report) for the model to Lewisham Homes.
- 3.55 “Deep-dive” discovery workshops and knowledge transfer, alongside operational alignment tasks, will take place to ensure that the migration of the Lewisham Homes datacentres to STS datacentres and the ongoing support of Lewisham Homes users will occur in a timely manner with as little risk as possible. The expected timeline for this is in June/July of this year.
- 3.56 It is likely that there will be TUPE implications to consider for both the shared services and for Lewisham Council.

Project Updates

- 3.57 STS have 61 In flight projects across Brent, Lewisham and Southwark.
- 3.58 To ensure that we manage the projects more effectively we meet with each borough on a monthly basis, at the project review meetings we go through the inflight projects, paying particular attention to the amber and red RAG status projects to ensure that the right focus and work collaboratively to unblock issues that may arise.
- 3.59 We also review all potential pipeline projects at the project review meetings, this is both STS and Council led projects, so we all have sight of what is potentially coming up stream and plan accordingly.
- 3.60 We are currently working on demand and capacity management tool to help with identifying where resources will be oversubscribed which will help with scheduling pipeline projects more accurately for both our own and our partner’s ongoing developments.
- 3.61 The Cloud programme after successfully completing Foundation phase in Summer 2020 is now working only on the Southwark related work. As a result, Southwark requested taking over direct governance of the programme team, costs, and remaining workload. This work covers migration of those required business and infrastructure applications remaining in the Capita data centres

(DCs) along with secure decommissioning of this server estate.

- 3.62 Southwark has identified 49 business applications needing to be migrated. The programme team are now working closely with business owners to ensure these systems are still required with the migration work being managed by our Infosys (our strategic cloud partner). Migrations are underway, supported by detailed dialogue with business owners and application suppliers.
- 3.63 In addition, there are a total of 959 servers that must be securely decommissioned to complete the exit from Southwark's Capita DCs by September 2021.

Procurement Updates

- 3.64 O2 contract for Southwark: Formal documentation put together by O2 was initially unsatisfactory and did not match original pricing on which the award was based. This had to go back to O2's commercial team but is now resolved. It is expected that the agreement will be entered into by the end of February.
- 3.65 The MobileIron MDM contract for Brent and Lewisham has been renewed to 30 November 2021, allowing time for consolidating MDM on Microsoft InTune later in the year. When the consolidation happens, savings will be realised as the MobileIron contract will have ceased. The renewal cost was £57k.
- 3.66 An implementation partner for Brent's new Sitecore web content management system has been procured.
- 3.67 The Ricoh contract has now been varied, with the required amendments to the contract model that accommodate changes to ways of working due to Covid-19 and giving transparency of pricing that will enable savings to be identified if there are further changes in machine numbers.
- 3.68 A new contract for Countercept Managed Detection and Response has been procured, providing significantly increased device coverage with a slight reduction on the £170k annual cost of the previous contract. Contract is for three years (2 plus 1).
- 3.69 Two separate five-year contracts for the new backup solution have been procured, one for the solution itself and another for the MS Azure storage that it will require.
- 3.70 A new contract for ProofPoint email filtering and fraud defence has been procured, to 25/02/22.
- 3.71 A procurement of a new three-year contract for Forcepoint web filtering is underway.
- 3.72 Procurement options for the Microsoft "ramp" to E5 for Southwark re being explored. It is planned to take an award decision to Brent's Cabinet in May.

4. Financial Implications

- 4.1 The Shared Technology Service (STS) is forecasting an underspend of £2,418 for 2020-21, against a total budget of £14,477,314 (this excludes the £120k accrued income from 2019/20). The underspend is primarily due to investment cases covering identified revenue pressures.
- 4.2 The total budget of £14.48m is a combination of non-controllable expenditure of £7.75m and controllable expenditure (staffing and consultancy) of £6.73m.
- 4.3 STS continue to operate under the improved charging process with the consumable recharges and project costs being stripped out effectively. From April 2020 to January 2021, a total of £6.59m of recharges have been identified and accounted for. This significantly helps eliminate any budgetary pressure STS would have encountered if these costs were absorbed in the core budget.
- 4.4 This favourable financial position has developed due to several improved practices:
 - Financial reporting – monthly budget review and charging meetings with all partners
 - Clarity around licencing costs – material licences have been identified and have been built into the core 2020/21 budget
 - The Microsoft settlement being finalised, and year 2 funding being made available to cover this
 - Capital costs being correctly identified and treated taking away any revenue pressures
- 4.5 Additional funding was needed to respond to the Covid-19 situation, Brent £375,667, Lewisham £331,072 and Southwark £173,155.

5. Legal Implications

- 5.1 This report is for noting. Therefore, no specific legal implications arise from the report at this stage.
- 5.2 Brent Council hosts the Shared ICT Service, pursuant to the Local Government Act 1972, the Local Government Act 2000, the Localism Act 2011 and the Local Authorities (Arrangements for the Discharge of Functions) (England) Regulations 2012. These provisions allow one council to delegate one of its functions to another council as well as allowing two or more councils to discharge their functions jointly with the option of establishing a joint committee. Joint committees can in turn delegate functions to one or more officers of the councils concerned. Decisions of joint committees are binding on the participating councils. However, subject to the terms of the arrangement, the council retains the ability to discharge that function itself.

6. Equality Implications

- 6.1 During the current Covid-19 crisis, the Shared Service has always followed government and council guidelines and policy to ensure the safety of our officers. Those officers in vulnerable categories or caring for others who may be vulnerable have been working

from home at all times. We have maintained a small staff presence at the council head offices, and have provided appropriate PPE equipment along with social distancing measures at all times,

7. Consultation with Ward Members and Stakeholders

7.1 There are none.

8. Human Resources/Property Implications (if appropriate)

8.1 The Target Operating Model will indicate the need for a future restructure of the service, this will be presented with a business case by the Managing Director.

Report sign off:

PETER GADSDON

Strategic Director of Customer &
Digital Services



Shared ICT Services Joint Committee Performance Pack

2nd March 2021



Joint Committee Performance Pack

Meeting Information

	Meeting Date and Time	Tuesday 2 nd March 2021 18:00 – 19:30
	Meeting Location	To be held online
	Dial-in Details	Online Meetings



Performance Management

Key Performance Indicators

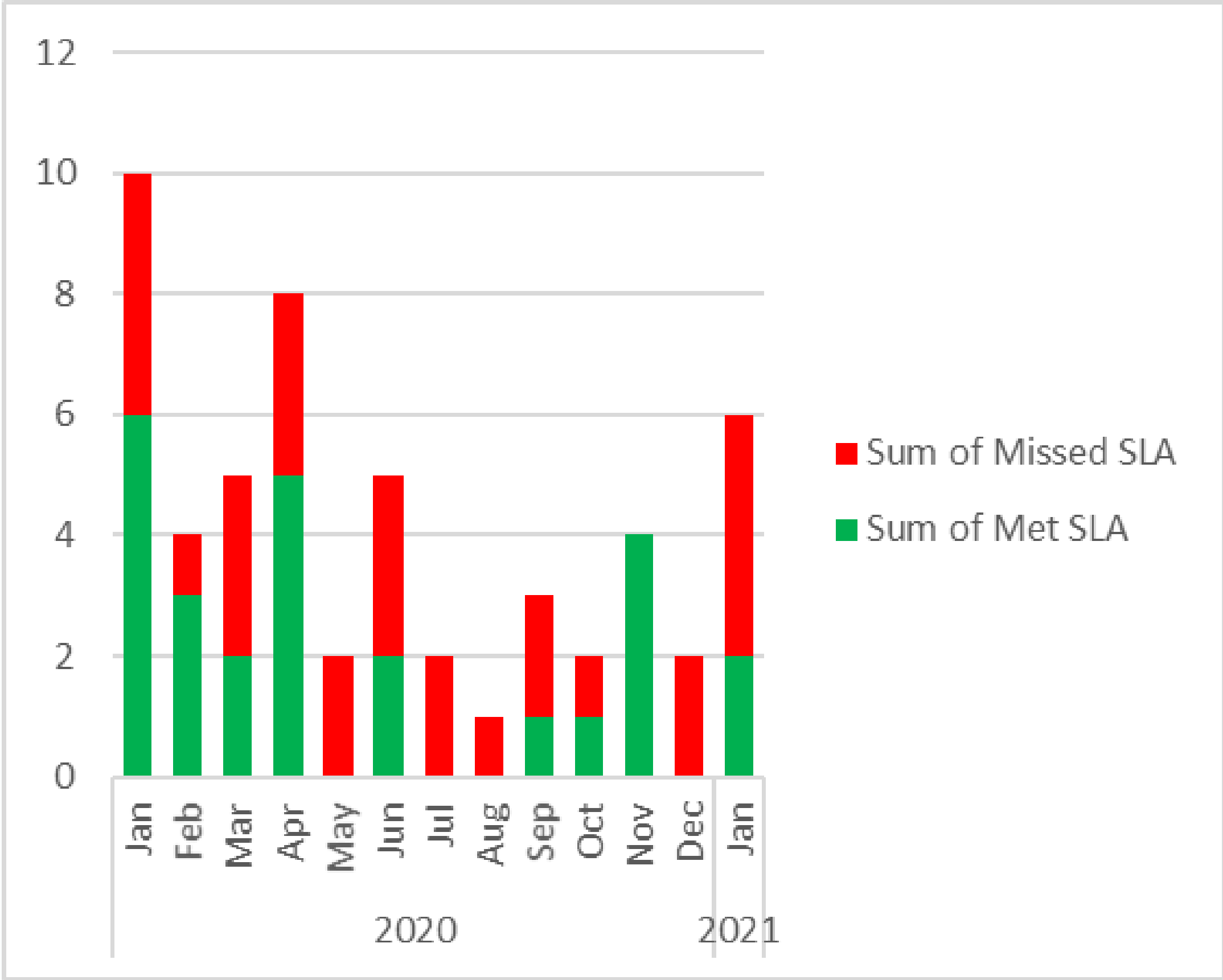
Summary

- P1 incidents increased primarily due to a total of 7 Council Public Web Site outages for Lewisham and Southwark
- P2, P3 and P4 SLA have all improved in this period compared with the last report due to improved call management
- Laptop Direct Access remote connection numbers have increased in Southwark as laptop rollout considerably accelerated
- Net Promoter Score above 60% (excellent rating level is 50%)
- No major security incidents that affected the Shared Service - October through to January



Performance Management

SICTS P0 & P1 - target 95% of calls fixed within 4 hours



Row Labels	Sum of Met SLA	Sum of Missed SLA	Total	Percentage Met	Percentage Missed
2020	24	24	48	50%	50%
Jan	6	4	10	60%	40%
Feb	3	1	4	75%	25%
Mar	2	3	5	40%	60%
Apr	5	3	8	63%	38%
May	0	2	2	0%	100%
Jun	2	3	5	40%	60%
Jul	0	2	2	0%	100%
Aug	0	1	1	0%	100%
Sep	1	2	3	33%	67%
Oct	1	1	2	50%	50%
Nov	4	0	4	100%	0%
Dec	0	2	2	0%	100%
2021	2	4	6	33%	67%
Jan	2	4	6	33%	67%
Grand Total	26	28	54	48%	52%



Performance Management

SICTS P2 target - 95% of calls fixed within 8 hours

Tickets Report

Ticket information generated by information from SQL database

Resolved Date

01/10/2020 31/01/2021

Organisation

Multiple selections

Priority

P2

Team (groups)

SICTS

Team

All

ClosureCategory

All

Logged Date

01/10/2020 31/01/2021

22.99

Average Ticket Closure Time

(Blank)

Tickets on Hold

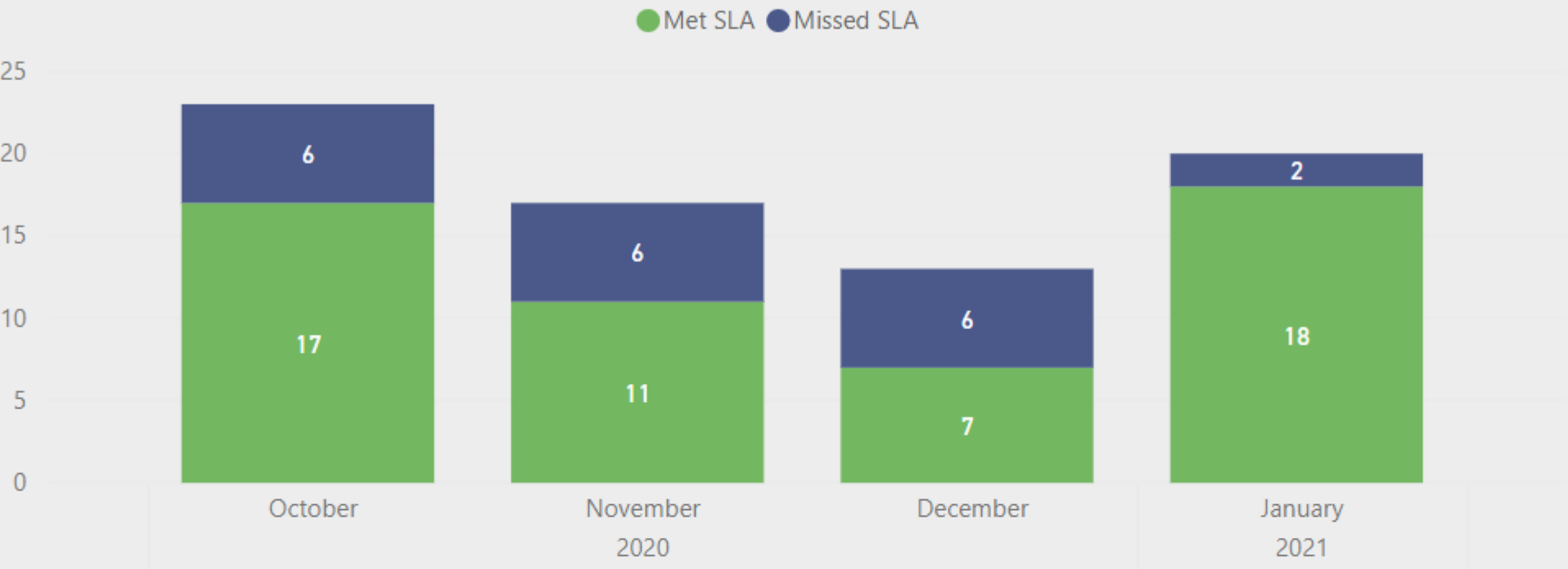
(Blank)

Reopened Tickets

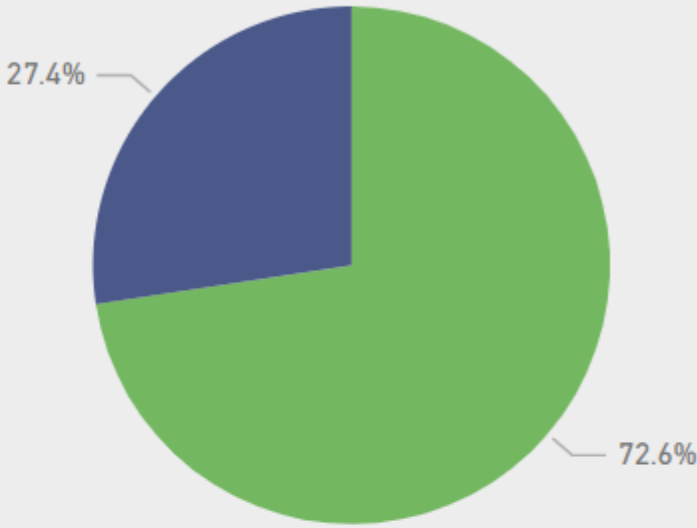
3

Open Tickets

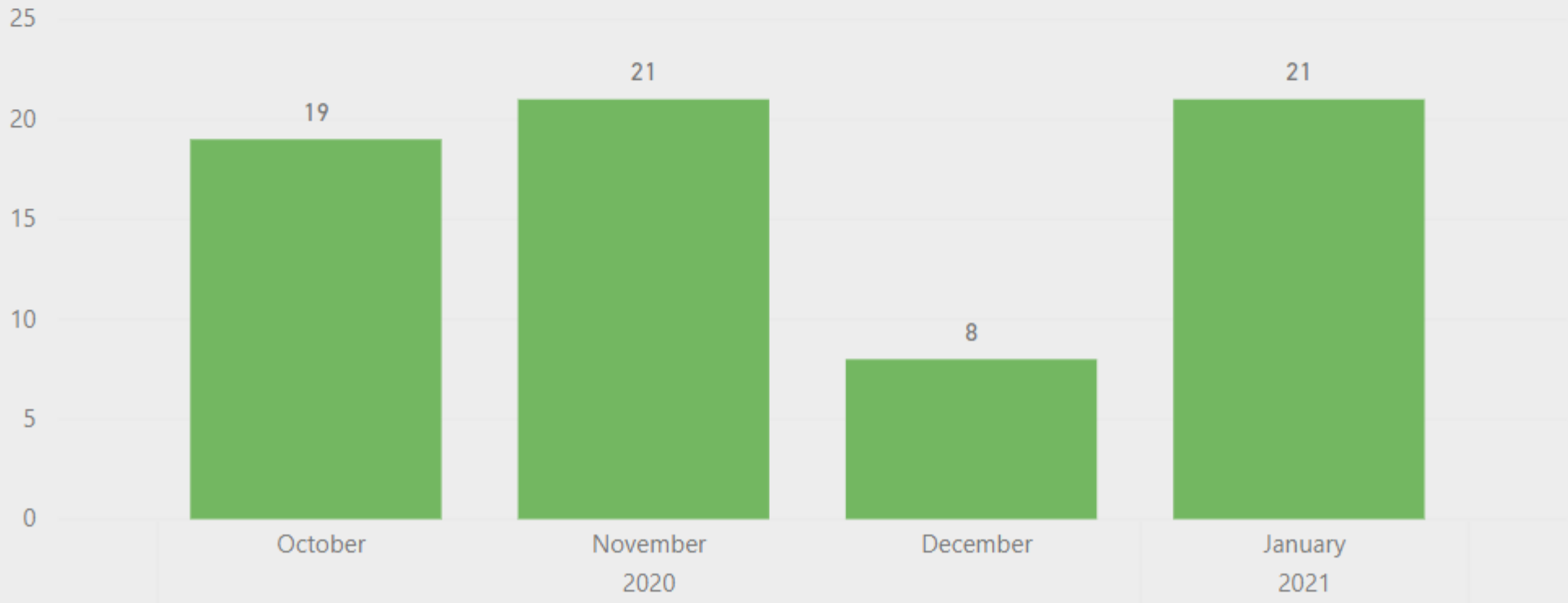
Tickets Resolved SLA Status



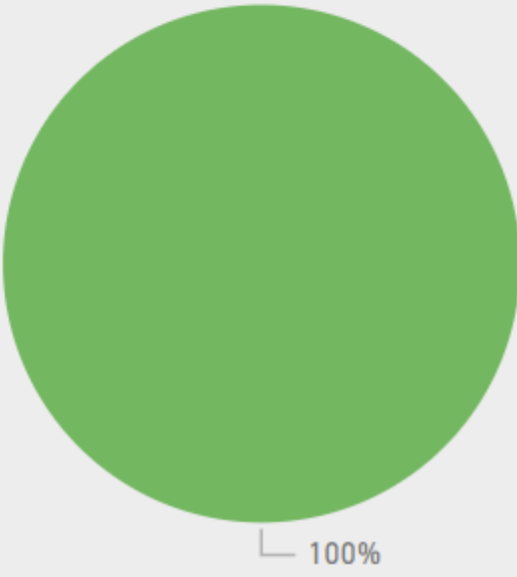
Percentage of Resolved Tickets by SLA Status



Tickets Logged



Percentage of Open Tickets by Status





Performance Management

SICTS P3 - target 80% of calls fixed within 2 working days





Performance Management

SICTS P4 - target 80% of calls fixed within SLA for request type





Performance Management – Net Promoter Score

Shared ICT Services

NPS scores

Tickets Report

Ticket information generated by information from SQL database

Organisation
Multiple selections

Date Range
01/10/2020 31/01/2021

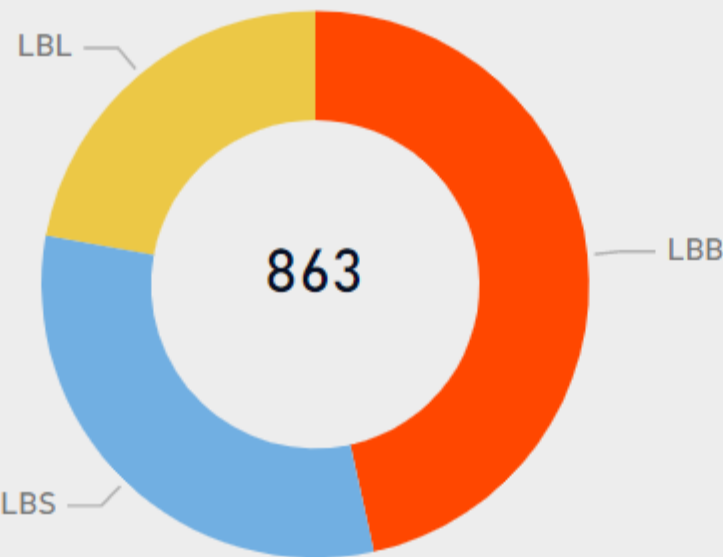
Team (groups)
SICTS

Team
All

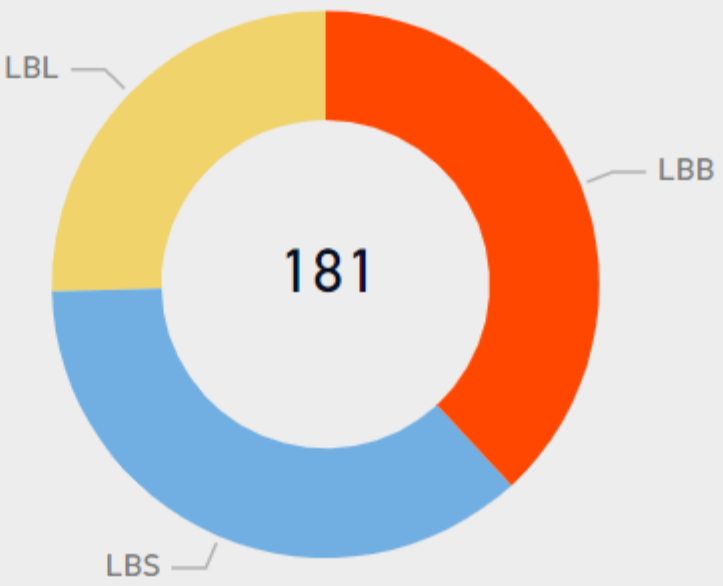
NPS Score
65.8%

npsValue

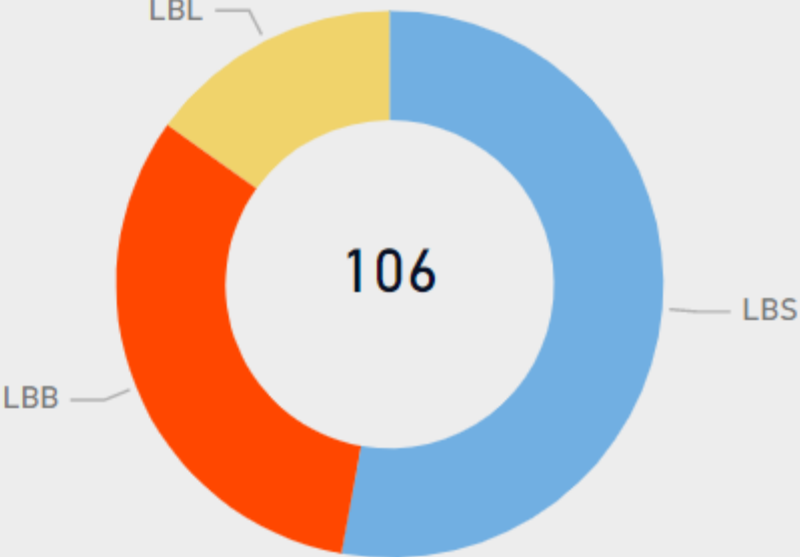
Promoters



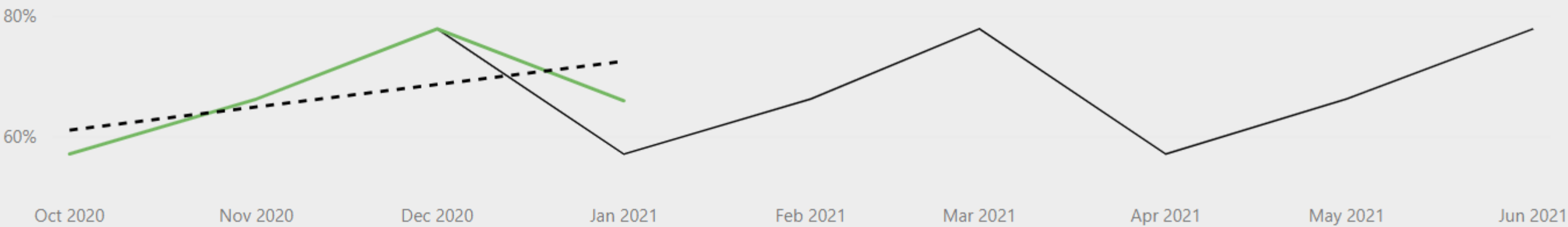
Passive



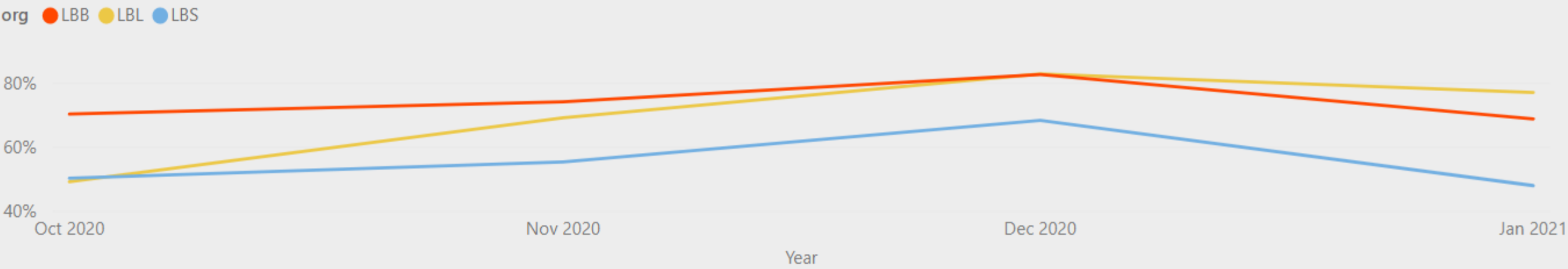
Detractors



NPS Score by Year and Month



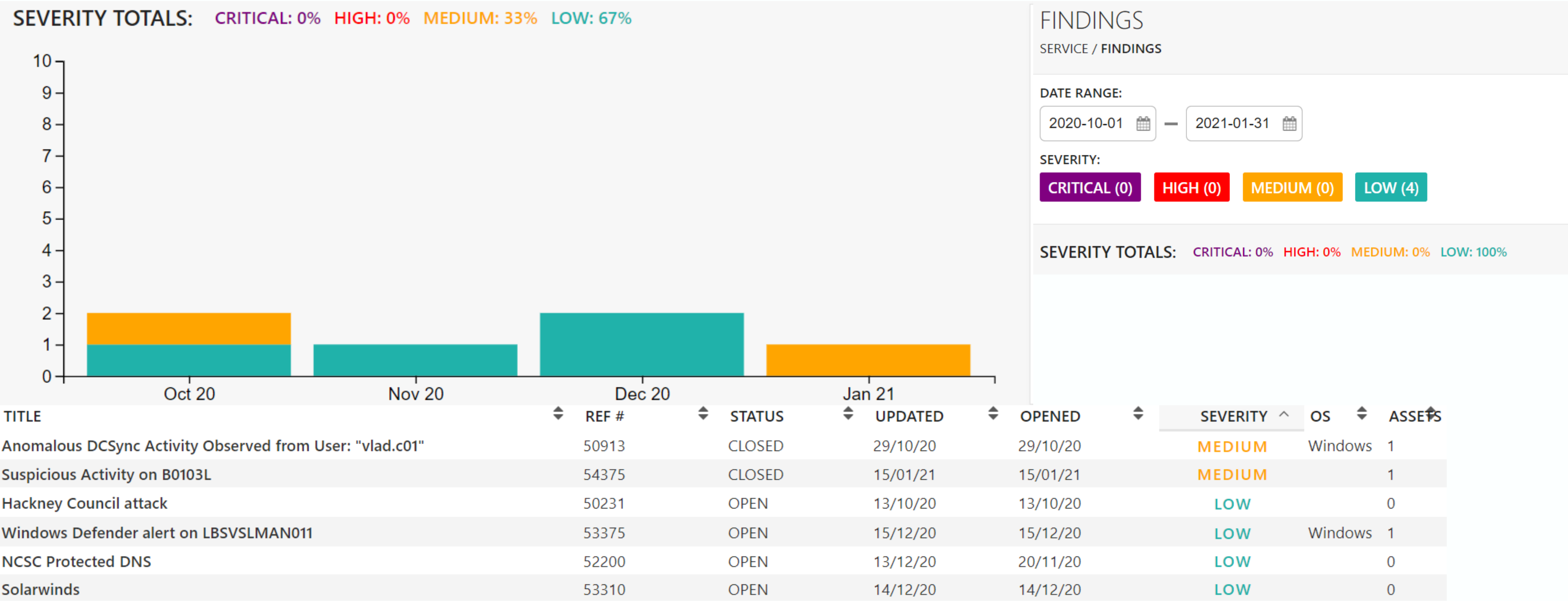
NPS Score by Year, Month and organisation





Performance Management

(Security Attack Incident Investigations)





Financial Update

Current financial outturn position

Category	Full Year			Year to Date	
	Budget	Forecast	Variance	Actuals	Remaining
ADVERTISING, PUBLICITY AND MARKETING	£ -	£ 8	£ -	£ 8	£ 8
FEES & CHARGES INCOME - OTHER	£ 595,125	£ 595,125	£ -	£ 495,938	£ 99,188
ICT HARDWARE	£ 25,000	£ 45,000	£ 20,000	£ 35,740	£ 10,740
ICT MAINTENANCE AND SUPPORT	£ 6,064,705	£ 4,058,440	£ 2,30,360	£ 1,983,442	£ 1,490,868
ICT SOFTWARE		£ 1,775,905		£ 2,590,395	
INTERNAL RECHARGES	£ 595,125	£ 595,125	£ -	£ 495,938	£ 99,188
INTERNET COSTS	£ 210,055	£ 222,000	£ 11,945	£ 184,841	£ 25,214
LAND LINE TELEPHONE COSTS	£ 819,775	£ 920,000	£ 100,225	£ 915,081	£ 95,306
MISCELLANEOUS EXPENSES	£ 68,007	£ -	£ 68,007	£ -	£ 68,007
MOBILE PHONE COSTS	£ 386,400	£ 436,920	£ 50,520	£ 429,583	£ 43,183
POSTAGE AND COURIER SERVICES	£ 20,000	£ 20,000	£ -	£ 17,209	£ 2,791
PURCHASE - EQUIPMENT, FURNITURE AND MATERIALS	£ -	£ 5,000	£ 5,000	£ 3,857	£ 3,857
PRINTING	£ 165,473	£ 101,490	£ 63,983	£ 32,368	£ 133,105
STORAGE AND ARCHIVING	£ 25,000	£ 17,000	£ 8,000	£ 15,689	£ 9,311
SUPPLIES & SERVICES RECHARGE	£ -	£ 2,000	£ 2,000	£ 1,650	£ 1,650
FACILITIES MANAGEMENT	£ -	£ 647	£ 647	£ 647	£ 647
NON-STAFF TRAINING	£ -	£ 500	£ 500	£ 483	£ 483
SUBSISTENCE	£ -	£ 2,000	£ 2,000	£ 1,428	£ 1,428
GROUNDS MAINTENANCE	£ -	£ 50	£ 50	£ 40	£ 40
HOTEL AND OTHER ACCOMMODATION COSTS	£ -	£ 500	£ 500	£ 271	£ 271
PHOTOCOPYING	£ -	£ 500	£ 500	£ 285	£ 285
RECHARGES - INCOME FROM OTHER	£ 287,193	£ 237,530	£ 49,663	£ 237,530	£ 49,663
STATIONERY	£ -	£ 500	£ 500	£ 256	£ 256
Total Expenditure	£ 7,497,222	£ 7,369,620	£ 127,594	£ 5,971,577	£ 1,525,645
CAR ALLOWANCES	£ -	£ 500	£ 500	£ 475	£ 475
SALARIES	£ 2,934,510	£ 2,701,749	£ 232,761	£ 2,211,409	£ 713,101
AGENCY STAFF	£ 1,134,729	£ 1,706,127	£ 581,398	£ 1,351,235	£ 226,496
CONSULTANCY FEES	£ 564,327	£ 266,473	£ 297,854	£ 199,855	£ 364,472
NATIONAL INSURANCE - EMPLOYERS CONTRIBUTION	£ 324,273	£ 311,525	£ 12,748	£ 261,718	£ 62,555
PENSIONS - EMPLOYERS CONTRIBUTION	£ 962,112	£ 945,825	£ 16,487	£ 792,092	£ 170,020
OVERTIME	£ 227,833	£ 157,000	£ 70,833	£ 125,347	£ 102,486
STAFF DEVELOPMENT AND TRAINING	£ 80,000	£ 35,000	£ 45,000	£ 32,725	£ 47,275
STATUTORY MATERNITY AND PATERNITY PAY	£ 6,000	£ -	£ 6,000	£ -	£ 6,000
STAFF RECRUITMENT COSTS	£ 25,000	£ 12,000	£ 13,000	£ 10,334	£ 14,666
STAFF DISCRETIONARY AWARDS	£ -	£ 12,500	£ 12,500	£ 11,862	£ 11,862
STATUTORY SICK PAY	£ 15,000	£ 1,000	£ 14,000	£ 899	£ 14,101
PUBLIC TRANSPORT FOR STAFF	£ -	£ 1,000	£ 1,000	£ 871	£ 871
MEMBERSHIP AND SUBSCRIPTIONS	£ -	£ 8	£ 8	£ 8	£ 8
TRANSPORT COSTS - STAFF	£ -	£ 750	£ 750	£ 508	£ 508
STAFF OTHER EXPENSES	£ -	£ 100	£ 100	£ 50	£ 50
Total BAU Staffing	£ 6,253,784	£ 6,151,341	£ 102,543	£ 4,999,313	£ 1,254,471
SICTS PROJECTS	£ 472,111	£ 472,111	£ -	£ 230,134	£ 241,977
Total Project Costs	£ 472,111	£ 472,111	£ -	£ 230,134	£ 241,977
Contingency Pot	£ 254,197	£ 254,197	£ -	£ 174,962	£ 79,235
Total Contingency Pot	£ 254,197	£ 254,197	£ -	£ 174,962	£ 79,235
Historic Croydon DC charge	£ 120,000	£ 347,719	£ 227,719	£ 337,000	£ 217,000
Total Service Charge	£ 14,597,314	£ 14,594,988	£ 2,418	£ 11,712,986	£ 2,884,328

Summary

The table shows the financial position for the whole of the shared service; individual authorities will receive their own monthly charges which will also outline their current financial position.

YTD current spend is £11.7m against a full year budget of £14.60m (this bottom line now includes the £120k accrued from 2019/20 for the Croydon DC charge). The current YTD spend excludes the £6.59m recharges that have been stripped out (e.g. cloud program costs, the XMA orders for the smart working project in Southwark and the smart tech project in Lewisham and the rechargeable bulk printing charges).

STS are currently forecasting a £2.4k underspend which takes into consideration all recharges being accounted for and the YTD Covid-19 spend of £874k being funded separately.



YTD Covid-19 Costs

Shared ICT Services

Organisation	Category	Mar - Nov
Brent	Courier service	6,555
	Equipment	107,974
	Mobile telephony	123,403
	printing	10,266
	Software Licence	57,651
	Staffing	14,400
Brent Total		320,250
Lewisham	Courier service	372
	Equipment	204,992
	Mobile telephony	83,295
	Software Licence	10,061
	Staffing	17,823
Lewisham Total		316,543
Southwark	Courier service	19,407
	Equipment	54,480
	Software Licence	66,154
	Staffing	27,423
Southwark Total		167,464
Grand Total		804,256

December	January	February
637	3,196	328
80	-	-
6,552	6,552	6,552
-	-	-
-	-	25,521
-	-	-
7,269	9,748	32,401
79	706	445
-	-	-
4,433	4,433	4,493
-	-	-
-	-	-
4,512	5,139	4,938
1,872	1,555	2,264
-	-	-
-	-	-
-	-	-
1,872	1,555	2,264
13,653	16,442	39,603

Grand Total
10,716
108,054
143,059
10,266
83,172
14,400
369,668
1,602
204,992
96,654
10,061
17,823
331,132
25,098
54,480
66,154
27,423
173,155
873,955

Summary

All partners have been emailed their latest Covid-19 costs which shows the detail behind the net total figures.

Current Covid-19 expenditure across the three partners is £874k.

All partners have now confirmed their own cost code (strategy) of dealing with these costs. At the monthly charging review meetings Covid-19 costs are highlighted and recharged to their own separate funding pot.



Risk Management

Key Financial Risks

Risk and Trend (cause, event, consequence)	Recent developments, progress and concerns	Impact	Probability	Priority	Actions
CPI/RPI/Exchange rate issues – potentially related to EU withdrawal or other global financial impacts.	Based on past experience, in particular where supplies and services are sourced from the USA, pricing can be particularly sensitive to exchange rate fluctuations. All contracts let indicate whether they are subject to indexation or not and these will be reviewed for the coming financial year.	3	3	9	Build indexation into budget forecast.
Lack of service maturity around cloud management could see unexpected costs.	The search for a cloud management tool is being conducted and relevant training is being identified.	3	4	12	Tool to be procured via the Tech Roadmap and training to be provided along side the implementation of the target operating model. Processes to be created for staff.
Base budget insufficient to meet service demands – potentially stems from being a new service with untested service model.	An initial target operating model has been drafted, and is now being reviewed along with the restructure to ensure alignment with business objectives. A review of the future 3-5 Year roadmap is underway and impacts of capital and revenue expenditure.	3	3	9	The Target Operating Model is being reviewed to ensure alignment with business and strategic objectives and requirements.
Unknown or unplanned expenditure may arise from licence shortfalls, warranty or maintenance contracts or changes to service use or growth.	Due diligence was undertaken when partner services were on-boarded however information is considered in part to be of poor quality. Were undertaking a further exercise to identify such information issues and will include the outcome of this work in our reporting. The councils’ central finance teams should note risk to base budget and consider contingency mechanism.	3	4	12	Risk to be monitored



Risk Management

Resourcing Risks

Risk and Trend (cause, event, consequence)	Recent developments, progress and concerns	Impact	Probability	Priority	Actions
Underlying imbalance between service demand and resource levels.	Imbalance is being met with agency staff, impact is continuity of staffing, knowledge and expertise.	4	3	12	New target operating model currently being implemented.
Unable to recruit/retain/afford sufficient skilled and qualified staff to run the service.	The target operating model will look to address the concerns, but it's a common issue where IT salaries to not match local government pay scales.	4	4	16	New target operating model currently being implemented.
Service fails to meet SLA targets.	Staff overtime is offered but not always taken up due to workloads during the normal day.	4	3	12	A review of SLA's were approved by the Joint Committee on the 18 th of Jan and the implementation of the new service will add additional support.
Projects delayed with subsequent business impact (potential loss of benefits and or financial cost).	Work to develop Project Management Office – formal project management with fully costed project delivery funded by the business.	4	3	12	Creation of the PMO build a pipeline of projects and align with council priorities.
Sub-optimal service delivery has both financial and reputational implications for the service and wider business.	Review of all process, introduction of the SICTS PMO and Technology Road Map to build our forward plan whilst rightsizing the service with the Target Operating Model.	4	3	12	Implement PMO, Technology Roadmap and Target Operating Model



Risk Management

Loss of service Risks

Risk and Trend (cause, event, consequence)	Recent developments, progress and concerns	Impact	Probability	Priority	Actions
Hardware, software or 3rd party service failure (eg: .Network goes down, power failure, telephony failure)	SICTS BC Plan has been reviewed and rewritten. Covid-19 crisis highlighted our BCP capability with over 7,000 users working remotely from March onwards We hold regular service review meetings with our partners (e.g. 8x8, Virgin Media, Risual, Liberty, Dell)	4	3	12	-Move to cloud-based computing will aid in the reduction of levels of infrastructure. - DR tests to be scheduled and reviewed
Malicious cyber activity impacting ability of ICT services to function normally. (eg: Denial of service attack).	-External review and internal audit of BCP completed. -Initials workshop held to identify gaps prior to audit.	4	4	16	-SICTS are attempting to consolidate the Cyber audits into one. -A Cyber Defence roadmap is being produced to harden the council's infrastructure.
Loss or severe impact to ICT service delivery. SICTS unable to deliver underpinning core ICT services to agreed SLA.	Work in progress to increase core infrastructure resilience and BC/DR exercises to be scheduled.	4	4	12	-Rollout of laptops will aid in the reduction of levels of infrastructure. -Now Covid-19 first wave has passed, DR Tests to be scheduled for various elements of the infrastructure
Staff (business) unable to access critical ICT services/systems	Brent and Lewisham and Southwark move to laptops supports home and remote working and reduces reliance on council offices to access services. Line of business applications migrating to Cloud will reduce reliance on SICTS infrastructure.	4	4	12	-DR plans being tested via desk-based activities. BCP invoked for all three councils during Covid-19 crisis.
Loss of public facing service provision and communication with residents.	Work required to formalise SICTS response to malicious activity and technical disruptions.	4	4	12	-Review processes with the business for communications.



Risk Management

Supportability Risks

Risk and Trend (cause, event, consequence)	Recent developments, progress and concerns	Impact	Probability	Priority	Actions
<ul style="list-style-type: none">• A continued reliance upon legacy systems (hardware, software).• In many cases upgrade or replacement of legacy systems will be dependent upon business led demand, resource, support and funding.• Lack of succession planning and funding for services.• Legacy systems are increasingly difficult and costly to support.• 3rd party support where required may cease.• Hardware spares may be unavailable.• Technical skills to support may become increasing scarce.• The business may fail to understand the issues with legacy support and fail to plan, budget and evolve accordingly.• Although this is a business risk it often becomes an ICT issue.• Increased cost and effort to support.• Product compatibility issues.• Constraining impact upon ICT and other business areas to adopt more modern technology and ways of working.	<p>Work in progress to develop technology roadmaps and service plans to support longer term (proactive) planning.</p> <p>Service account managers working within the business to identify and resolve issues where these are identified.</p> <p>Where required, sourcing of appropriate contracts to extend service life support.</p> <p>Full network scanning now in place.</p> <p>Windows 2008 Support Arrangements</p> <ul style="list-style-type: none">-Brent has purchased extended for one year-Lewisham has purchased extended support for one year excluding the RDS estate-Southwark has purchased extended support	3	5	15	<p>Technology Road map and strategies in place, funding to be requested at council capital boards.</p> <p>Investment cases to be produced to gain funding.</p> <p>Reduction in the level of infrastructure and move to the cloud to mitigate legacy hardware</p> <p>Move to laptop estate and implementation of a Windows servicing plan to address end user computing OS level risks.</p>



Shared ICT Services

Thank You



DATA CENTRE (DC) MIGRATION PROGRAMME – Applications Lift & Shift Plan (Feb 2021)

1

SharedTechnology Services

Data Centre Migration – Outline Plan

Milestone	Planned Date	Actual Start Date	Slippage
Start Server Decommissioning	1 Dec 2020	1 Dec 2020	None
Start Infrastructure Application Migrations	8 Dec 2020	8 Dec 2020	None
Start Business Apps Migrations	20 Dec 2020	16 Dec 2020	None
Complete Business Apps Migration	31 July 2021	NA	None
Complete Infrastructure App Migrations	01 Sep 2021	NA	None
Complete Server Decommissioning	14 Sep 2021	NA	None
Start Secure Destruction of Hardware in Capita DCs	15 Sep 2021	NA	None
Physical Exit from Capita DCs	30 Sept 2021	NA	None
Complete Decommission of Tooley Street DC	31 Oct 2021	NA	None



DC MIGRATION PROGRAMME – Applications Lift & Shift Plan (Feb 2021)

SharedTechnology Services

Business Applications: Outline Schedule

Batch	Business Application (Area)
1 Dec '20 Completed	<ul style="list-style-type: none">Southwark Web SystemsHavenstar
2 & 3 Feb '21	<ul style="list-style-type: none">Croydon Pest Control (Traded Services)Qmatic (Housing)BACS Payments (Exchequer)MobileFrame (Traded Services)iCaseWork (Planning)HRCasework (HR)TMO Database (Highways)Soti MobiControl (Traded Services)
4 Mar '21	<ul style="list-style-type: none">3M Conversion (Libraries)eMuseum (Museums/Libraries)TMS Collections (Museums/Libraries)Deep Freeze (Libraries)Netloan (Libraries)SuperNova (Libraries)Modern.Gov (Constitutional)

Batch	Business Application
5 Apr '21	<ul style="list-style-type: none">CYP Directory – FID (ChAd)iDox Children's (ChAd)Mosaic (ChAd)MASH Maisy (ChAd)CareStore (ChAd)
6 May '21	<ul style="list-style-type: none">ASC Policy & Procedures (ChAd)Spectrum Spatial Analyst (Corp GIS)Atracs (FM)Apex (Asset Management)
7 June '21	<ul style="list-style-type: none">Jontek Answerlink (Contact Centre)VisualFiles (Legal)Zylpha Docbinder (Legal)Intranet (Comms)
8 July '21	<ul style="list-style-type: none">BACAS NG (Cemeteries)Xpress (Electoral Services)Coroners (Coroners/Registration)



DC MIGRATION PROGRAMME – Applications Lift & Shift Plan (Feb 2021)

Business Applications – Decommission with dependenc

Batch	Application (Dept)	Comments
Decommission Group	<ul style="list-style-type: none">NBS Building (Chief Exec)Revs & Bens Info@Work (Finance)AIM (Finance)Business Objects (ChAd)MS Dynamics (Housing & Mod)CareWorks (ChAd)Impact Response (Housing & Mod)	<ul style="list-style-type: none">Dependent on separate business migration by May 2021Dependent on separate business migration by May 2021Dependent on separate Cloud migration to Capita hosted servicePost CareFirst move to hosted platformDependent on Hitachi engagementClarifying with business their need to access old recordsBusiness moving to new housing repairs supplier – remove when in place

Note:
This is a list of business applications with known dependencies affecting when they can be decommissioned. It is likely to increase with further business areas engagement when confirming switch off dates



DC MIGRATION PROGRAMME – Applications Lift & Shift Plan (Feb 2021)

SharedTechnology Services

Infrastructure Applications – Batches 1 - 3

Batch	Infrastructure Application
<div>1</div> <div>In progress</div>	<ul style="list-style-type: none">• Legacy Backups• NetBackup• MS Intune• Exchange 2010• Exchange 2003• Libraries VPN• Netcall• Jontek ISDN• Northgate Circuits - Completed

Batch	Infrastructure Application
<div>2</div> <div>Continued</div>	<ul style="list-style-type: none">• SolarWinds NPM• SAP/COLT• N3 (Cody)• Site-to-Site VPN• MOBEX• DHCP• Internal DNS• NTP• Dedicated Print Queues• Azure AD Connect• MS SCOM

Batch	Infrastructure Application
<div>2</div>	<ul style="list-style-type: none">• Avaya• Central Print Queues• SCCM• Active Directory• ADFS

Batch	Infrastructure Application
<div>3</div>	<ul style="list-style-type: none">• APPV• Dedicated Windows File Servers• DDOS Spring

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		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. 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	£1.68m		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	£0.12m		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	£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.

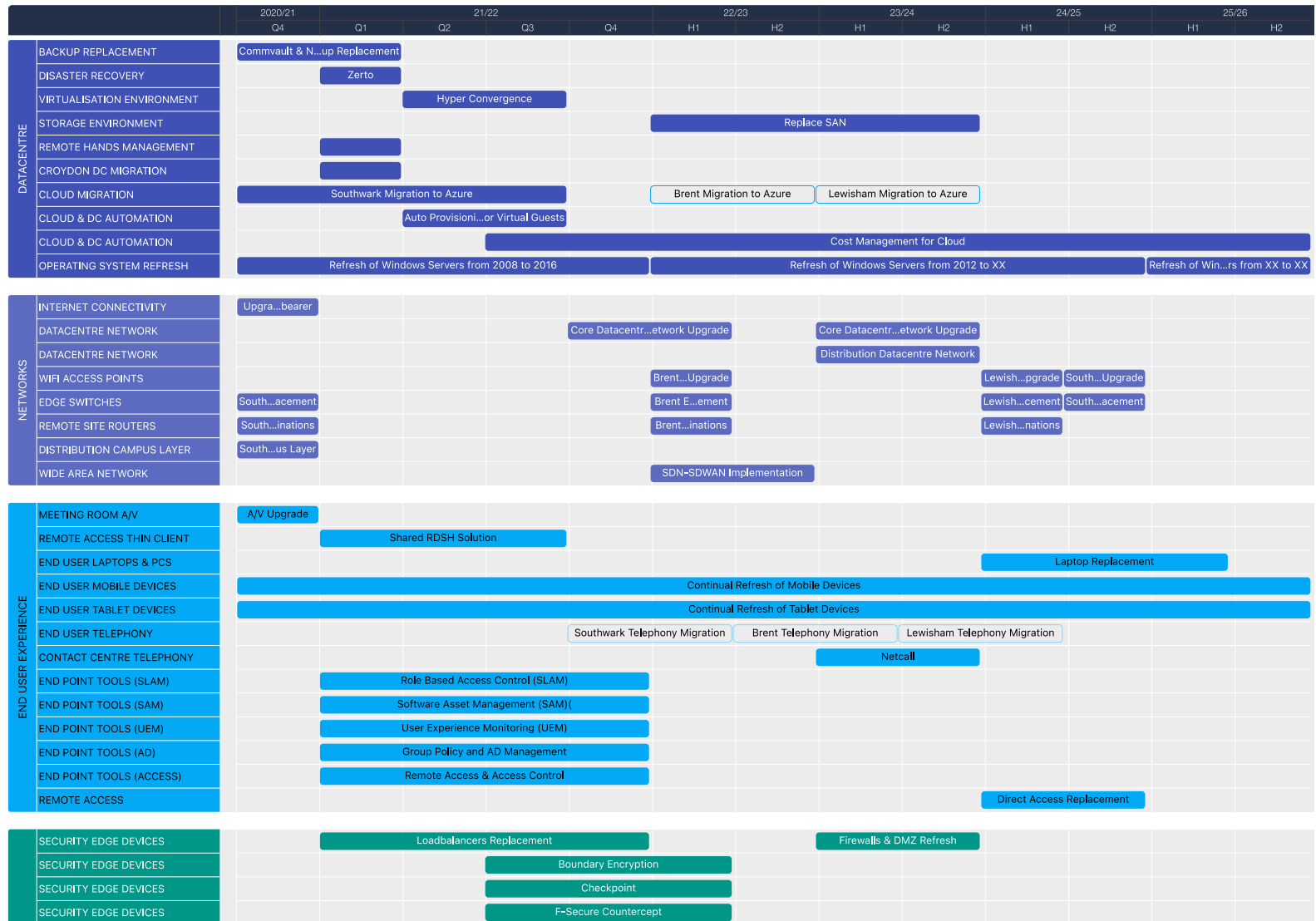
We will ensure that the services that we provide and the mechanism of accessing them are easy to use, intuitive and appropriate for each role.”

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		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	£0.14m		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).
Staff technical training	£0.08m		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.

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	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																				



February 2021

Created by:

Tim Green – Senior Programme Manager

Jason Carney – Enterprise Architect

Kevin Ginn – Head of Operations

Shared Technology Services Cyber Security Strategy 2021-2024

THE CHALLENGE

In a world of electronic information, the protection of our data is becoming ever more important. The amalgamation of data stored in smart watches to the far stretched 'misunderstood' cloud means we don't understand the footprint and trail our data leaves behind.

We exist in a culture powered by interconnecting data, constantly evolving and allowing us to make better decisions. We experience the benefits of this in public sector but due to our need and want to share, we create a weakening around our control of the data. Once it has left our environment and spreads out into other infrastructure the legislation, we use to govern our data may no longer have application.

This makes it even more critical for us to put in controls around how we use, store and process our data. It makes it critical for us to follow the guidance from the experts and to ensure that our systems are appropriately hardened and locked down to keep the attackers out and our systems continuously working well.

The real challenge comes when there is a need to encourage more collaboration, more access to information and to encourage transformation within an organisation. Very often, the rules around responsible data management stifles the ability to share. One of the most difficult jobs in this area is to effectively balance and enable transformation but also to continue the responsible use of data that we are accountable for.

Cyber incidents are on the rise, especially within public sector. We know that the ramifications are serious and widespread, from personal to economic. Protection and remediation are service disrupting and of significant financial expense. The impact on people affected by their stolen information can be disturbing and life altering in some cases.

This Cyber Security strategy outlines the focus we shall be adopting for our councils and customers. It is imperative that we put the right controls in place to protect and react to cyber threats going forward. We have a strong relationship with National Cyber Security Centre and other private cyber agencies which we will harness to help us to protect the data of our citizens and our customers.

We want to continue to use the benefits of technology to improve the lives of local people. This strategy will safeguard us all. It will build confidence in the way we operate and deliver our services and keep us at the forefront of the digital revolution.

INTRODUCTION

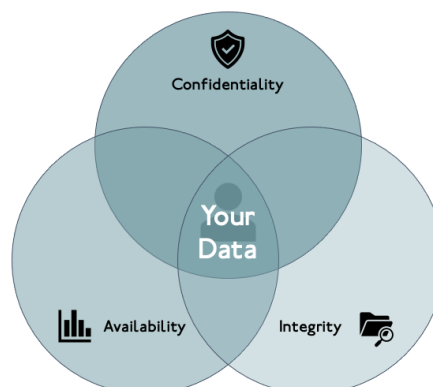
The Shared Technology Services (STS) is an IT shared service for the councils of Brent, Lewisham and Southwark. Brent council is the host borough for the service. STS is governed by a Inter Authority Agreement, a Joint Committee of two elected members from each council and the executive directors.

This document sets out the STS application of information and cyber security standards to protect our systems, the data held on them, and the services we provide from unauthorised access, harm or misuse. It is our cyber security commitment to the people we represent and is of national interest. It emphasises the importance of cyber security in the role of all staff.

WHY IS CYBER SECURITY IMPORTANT?

Cyber security is the practice of ensuring the confidentiality, integrity and availability (CIA) of information.

- Attacks on Confidentiality – stealing, or rather copying personal information.
- Attacks on Integrity – seeks to corrupt, damage or destroy information or systems and the people who rely on them.
- Attacks on Availability – denial of services, seen in the form of ransomware.



Cyber security refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorised access. Cyber security may also be referred to as information technology security.

Cyber security is important because, in order to effectively deliver services, we all process and store large amounts of data on computers and other devices. A significant portion of this data is sensitive information. It includes financial data, personal information and other types of data for which unauthorised access or exposure could have negative consequences.

We transmit sensitive data across networks and to other devices in the course of providing services or even just using your mobile to look at social media. Cyber security is the discipline dedicated to protecting this information and the systems used to process or store it. It is everyone's responsibility to ensure that we manage our data appropriately.

Cyber security is crucial in ensuring our services are kept up and running. It is also vital in ensuring in building and keeping our public's trust. A cyber-attack would have very serious consequences both in terms of a disruption to our services (many of which serve some of our most vulnerable residents), council's reputation and impact to our fiscal position.

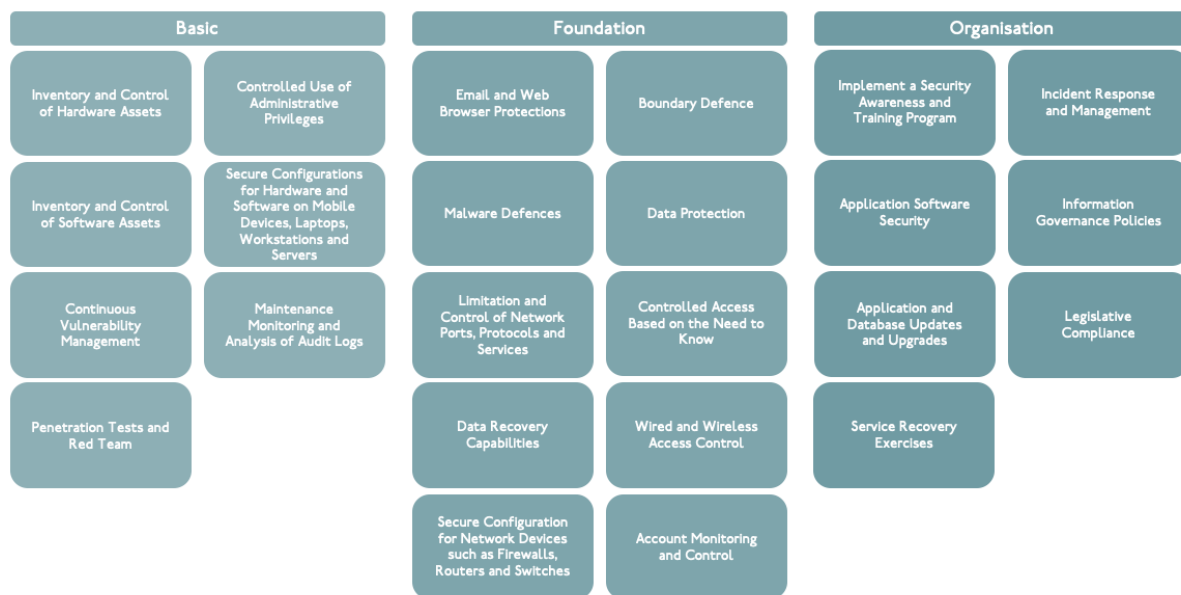
PURPOSE AND SCOPE

STS seeks to enable its partners to deliver its corporate and digital strategies, it is required that we allow our organisations to navigate cyber obstacles. The scale of transformation represents an unprecedented culture shift for staff, residents, partners and businesses. This in turn creates risk.

The Cyber Security Strategy is a new strategy introduced in response to several successful and high-profile cyber-attacks on public and private organisations. The purpose of the strategy is to give assurance to our councils and customers and to explain our commitment in delivering robust information security measures.

Through delivery of this strategy, we will comply with and embed the principles of 'Cyber Essentials'; a government-backed, industry-supported scheme to help organisations protect themselves against common online threats.

This strategy is intended to cover all partners and customers, the data on the systems we are responsible for, and the services they help provide. The recommendations in this strategy will be embedded in all areas of new and emerging technologies which we implement. It will also set out the best practices that will be rooted in our business as usual.



ASSETS

STS will regularly review the value of all assets across the partnership, ensure that political, social and economic values are considered to place the appropriate levels of protection around those digital and physical assets. Our assets:

- Data
- Services
- Infrastructure

VULNERABILITIES

Vulnerabilities are weaknesses or other conditions in an organisation that a threat actor; such as a hacker, nation-state, disgruntled employee, or other attacker, can exploit to adversely affect data security.

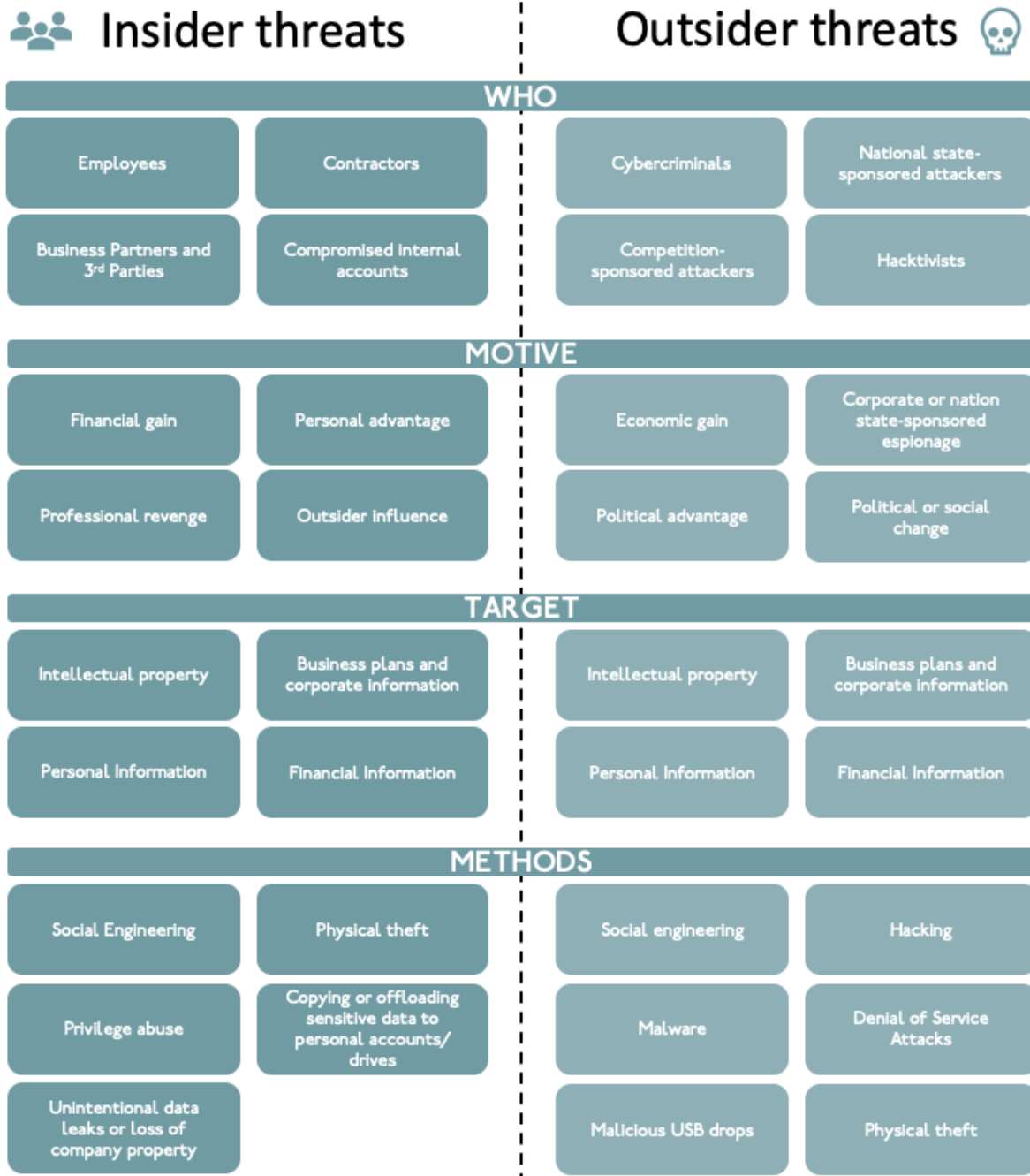
Cyber vulnerabilities typically include a subset of those weaknesses and focus on issues in the IT software, hardware, and systems an organisation uses.

- System Maintenance – IT systems should be updated and checked regularly and effectively. It is essential that the systems are fully updated and appropriate fixes are applied. Poor setup, mismanagement or other issues in the way an organisation installs and maintains its IT hardware and software components is a threat.
- Legacy Software – To ensure that legacy systems have sufficient user and system authentication, data authenticity verification, or data integrity checking features that prevent uncontrolled access to systems.
- Trend Analysis - The monitoring of organisational working patterns to identify unusual behaviour and respond accordingly.
- Training and Skills – It is of paramount importance that all employees have a fundamental awareness of cyber security to support this.

THREATS

If left unchecked, a threat could disrupt the day-to-day operations, the delivery of local public services and ultimately has the potential to compromise national security.

Generally, there are two types of threats. Insider Threats or Outsider Threats they are explained in detail below.



-CYBERCRIMINALS

Generally, cybercriminals are working for financial gain. Most commonly, for the purposes of fraud either by selling illegally gained information to a third party or using directly for criminal means.

Key tools and methods used by cybercriminals include:

- Malware – malicious software that includes viruses, Trojans, worms or any code or content that could have an adverse impact on organisations or individuals
- Ransomware – a kind of malware that locks victims out of their data or systems and only allows access once money is paid

- Phishing – emails purporting to come from a public agency to extract sensitive information from members of the public.

-HACKTIVISM

Hacktivists will generally take over public websites or social media accounts to raise the profile of a particular cause.

When targeted against local government websites and networks, these attacks can cause local reputational damage. If online services are regularly disrupted by cyber-attacks this could lead to the erosion of public confidence in such services.

Hackivist groups have successfully used distributed denial of service attacks to disrupt the websites of a number of councils already. (DDoS attacks are when a system, service or network is burdened to such an extent by an electronic attack that it becomes unavailable).

-INSIDERS

Staff may intentionally or unintentionally release sensitive information or data into the public domain. This could be for the purpose of sabotage or in order to sell to another party, but more often than not it is due to simple human error or a lack of awareness about the particular risks involved.

Malicious insider threats may include privileged administrative groups.

-ZERO DAY THREATS

A zero-day exploit is a cyber-attack that occurs on the same day or before a weakness has been discovered in software. At that point, it's exploited before a fix becomes available from its creator. It is an attack that exploits a previously unknown security vulnerability.

This poses a risk to any computer or system that has not had the relevant patch applied or the relevant updates to its antivirus software.

-PHYSICAL THREATS

The increasing reliance on digital services brings with it an increased vulnerability in the event of a fire, flood, power failure or other disaster (natural or otherwise).

-TERRORISTS

Some terrorist groups demonstrate intent to conduct cyber-attacks, but fortunately have limited technical capability. Terrorist groups could obtain improved capability in a number of ways, namely through the sharing of expertise in online forums providing a significant opportunity for terrorists to escalate their capability.

-ESPIONAGE

Several of the most sophisticated and hostile foreign intelligence agencies target UK government and public sector networks to steal sensitive information. This could ultimately disadvantage the UK in diplomatic, trade or military negotiations.

RISKS

Cyber Risk Management is a fundamental part of the broader risk management to ensure cyber security challenges are fully identified across the councils and appropriate action is carried out to mitigate the risk but also develop effective recovery and containment procedures in the event of an incident.

A risk consists of a threat and a vulnerability of an asset.

OUR APPROACH

To mitigate the multiple threats, we face and safeguard our interests, we need a strategic approach that underpins our collective and individual actions in the digital domain over the next three years. This will include:

- Foster a culture of empowerment, accountability and continuous improvement.
- Prioritising information assets and processes with our councils and customers, maintaining a register and conducting regular reviews including data retention policies.
- Ensuring adequate plans are in place to recover and quickly identify exposure.
- A council wide risk management framework to help build a risk aware culture within each of the councils, ensuring staff understand how to identify and manage risks.
- Cyber Awareness training and principles to help mitigate insider threats, understand supply chain risks and ensure all staff understand the issues and their responsibilities.

The diagram below shows the continual cycle for protecting the councils and its customers for cyber-attacks:



To further enhance the maturity and capability of the service we will be building a Cyber Security team within the Shared Service, this will focus on the delivering the technical controls and guidance to the councils and customers of the Shared Service. This will be led by a new role the Chief Information Security Officer. April 2021 will see a new Target Operating Model start which will ensure that focus is given to the maturity and capacity of the council's defences.

IMPLEMENTATION PLAN

To adapt to the changing landscape and achieve our vision we will align with the National Cyber Security Strategy's approach to defend our, residents, councils and customers and deter our adversaries and to develop our capabilities.

It is recognised that each partner and council will be at different levels of maturity and capacity therefore STS has developed a 5-year (2021-2026) Technology Roadmap in which it will invest a significant number in cyber protections, look for opportunities where we can share, build and grow together but also react to different levels of risk appetite.

DEFEND

STS will have the means to defend against evolving cyber threats, to respond effectively to incidents, and to ensure networks, data and systems are protected and resilient. It includes helping our residents, businesses and partners in gaining the knowledge and ability to defend themselves.

Actions:

- Implementing daily firewalls and scanning services.
- Continue to email hygiene for all partners and enable Attack Targeted Prevention.
- Improve threat correlation and reporting services.
- Ensure vulnerability and patch management is kept up to date.
- Ensuring that Cyber Security is considered in any procurement of solutions.
- Work with councils and customers to ensure websites and line of business systems are kept secure.
- Continue with a 3rd party Security Operations Centre partner to give us the assurance and protection of our systems, using dynamic and Artificial Intelligence (AI) from across the global to identify immediate threats.
- Carrying out health checks, penetration test and cyber resilience exercises to test their systems and processes, e.g. Web Check – a website configuration and vulnerability scanning service, developed with a number of public sector organisations including councils. This is free to use and available to all public sector organisations.
- Identify an STS Red team to be able to respond to incidents and have relationships in place with government agencies and cyber specialists.
- Ensuring that we carryout regular backups and recovery exercises
- Meeting compliance regimes, Code of Connection (CoCo) which require good cyber hygiene, to connect to government private networks, e.g. Public Sector Network (PSN) and the Health and Social Care Network.
- Working with partners across the public sector through participation in Cyber Security Information Sharing Partnership (CiSP), Warning, Advice and Reporting.
- Comply with The Minimum Cyber Security Standard
- Comply with Data Protection Act 2018 (including the Applied General Data Protection Regulation EU679/2016) and the Freedom of Information Act 2000
- Comply with Section 224 of Local Government Act 1972
- Work towards ISO27001.
- Comply with Access to Health Record Act 1990 and Access to Personal Files Act 1987
- Comply with PCI-DSS requirements for taking electronic payments.

DETER

Our councils and customers will be a desirable target for all forms of aggression in cyberspace. This will involve detecting, understanding, investigating and disrupting hostile action against us.

Actions:

- Applying government's cyber security guidance, e.g. 10 Steps to Cyber Security or Cyber Essentials.
- Users with wide ranging or extensive system privilege shall not use their highly privileged accounts for high-risk functions, in particular reading email and web browsing.
- Multi-factor authentication shall be used where technically possible, such as where administrative consoles provide access to manage cloud based infrastructure, platforms or services. Multi - factor authentication shall be used for access to enterprise level social media accounts.
- Passwords for highly privileged system accounts, social media accounts and infrastructure components shall be changed from default values and shall not be easy to guess. Passwords which would on their own grant extensive system access, should have high complexity and introduce multi-factor authentication.
- Use of Malware prevention and ensure air gaps or immutable storage.
- Ensure removable media is encrypted to the last levels controls.
- Improve micro segmentation of the network to avoid attackers crossing the network.
- Secure configuration to avoid access to critical information and enabling attackers.
- Introduce cyber awareness and training for users to help detect, deter and defend against the cyber threats.

DEVELOP

This includes developing a co-ordinated and tailored approach to risks and threats that we may encounter and mitigate potential vulnerabilities.

Actions:

- Develop and maintain risk management framework, internal control and governance for the prevention and detection of irregularities and fraud
- Process, procedures and controls to manage changes in cyber threat level and vulnerabilities
- Managing vulnerabilities that may allow an attacker to gain access to critical systems
- Operation of the council's penetration testing programme; and Cyber-incident response
- Introducing training for staff and elected members
- Develop an incident response and management plan, with clearly defined actions, roles and responsibilities
- Develop a communication plan in the event of an incident which includes notifying (for example) the relevant supervisory body, senior accountable individuals, the Departmental press office, the National Cyber Security Centre (NCSC), Government Security Group (Cabinet Office), the Information Commissioner's Office (ICO) or law enforcement as applicable (not exhaustive)

- Develop a network of sharing with other councils and customers, collaborate and learn from each other, harness networks such as London Office of Technology and Innovation, London CIO council, WARP, IGfL and ISfL.

REACT

STS will ensure that we have the sufficient controls in place to respond to an attack and furthermore have the organisational channels and processes to make efficient decisions further protecting our data and limiting any scope of an attacker.

We have third parties proactively monitoring our environment disabling any potential threats and locking down resources which are identified as a risk.

SUCCESS FACTORS

Throughout this period of challenging transformation, the councils have committed to delivering robust information security measures to protect our data from misuse and cyber threats, and to safeguard their privacy through increasingly secure and modern information governance and data sharing arrangements both internally and with partners.

To continue to provide assurance on the effectiveness and robustness of STS's arrangements for IT security, we will:

- Develop appropriate cyber security governance processes
- Develop a Cyber Risk Management Framework
- Develop policies/procedures to review access on a regular basis
- Create a cyber-specific Business Continuity Management Plan and/or Incident Plan to include emergency planning for cyber attack
- Develop an incident response and management plan, with clearly defined actions, roles and responsibilities. A copy of all incidents shall be recorded regardless of the need to report them
- Set up a Playbook to have test incidents on a regular basis; to ensure reaction to incidents where an incident is triggered
- Create standard test plans with security testing as a standard
- Reconcile current systems in place and last times these were reviewed (build into Enterprise Architecture)
- Review vendor management – process of assessments of third parties
- Explore Active Cyber Defence tools and new technologies to ensure partners have the best solutions to match to threats
- Apply the governments cyber security guidance – 10 Steps to Cyber Security
- Provide relevant cyber security training for staff and elected members
- Apply a regular schedule of cyber exercises, within the wider cycle of multi-agency incident response and recovery exercises
- Comply with the Governments Public Sector Network (PSN) Code of Connection and Payment Card Industry (PCI) standards; a minimum requirement for all systems used, audit trails, deletion of data etc.
- Protect enterprise technology by working with specialist partners to develop model architecture and review audit logs to reduce chances of threats

ROLES AND RESPONSIBILITIES

Information Governance and Policy will remain the responsibility of the councils and customers and the Shared Service will work with those teams to ensure that shared understanding and collaboration is met.

Effective cyber security governance in STS is delivered through the following roles and functions.

Senior Information Risk Owner (SIRO)

A nominated Senior Information Risk Owner (SIRO) is responsible for the governance of cyber security and information risk within the Council. This includes ensuring that information governance risk is managed in accordance with GDPR.

However, whilst the SIRO is the nominated officer, responsibility for safeguarding information and information systems is shared across the organisation with all staff having a role to play.

Joint Committee (JC)

The Joint Committee is made up of the lead councillors for IT. The Joint Committee will sponsor the Cyber Security Strategy and oversee the strategic framework through which the council governs its information resources and in turn agree and receive updates on implementation of the Cyber Security Strategy.

Joint Management Board (JMB)

The Joint Management Board is responsible for the strategic direction of the shared service and is made up of the executive directors from each council and the Managing Director of the shared service. This board is responsible for holding the shared service to account on the delivery of its obligations in turn the protection of its data and systems.

Operational Management Board (OMB)

The Operational Management Board is responsible for the day-to-day tracking of tasks and deliverables, this board will allocate resources and funds necessary to deliver the protection to the councils and its customers. The board is made up of Heads of IT from each council and the Senior Leadership Team of the shared service.

Information Governance Group (IGG)

The IGG is comprised of senior representatives from each council area. The group are responsible for overseeing the delivery of the Cyber Security Strategy and monitoring its effectiveness.

Technical Design Authority (TDA)

The Technical Design Authority (TDA) make decisions regarding technical implementations for projects. This includes ensuring that cyber security implications are properly considered.

Information Asset Owners (IAO)

Information Asset Owners are responsible for all processing of personal data within their business area.

All council officers

It is the responsibility of all officers to comply with the standards set out in this Cyber Security Strategy

This page is intentionally blank