Public Document Pack

# SUMMONS AND AGENDA

# BRENT, LEWISHAM AND SOUTHWARK IT COMMITTEE

**Date:** **TUESDAY, 26 NOVEMBER 2024 at 6.00 pm**

**Southwark Council**
**Meeting room G01**
**160 Tooley Street**
**London SE1 2QH**

**Enquiries to:** **Abby Shinhmar – abby.shinhmar@brent.gov.uk**
**Telephone:** **020 8937 2078**

**MEMBERS**

Councillor Amanda De Ryk
Councillor James-J Walsh
Councillor Fleur Donnelly-Jackson
Councillor Mili Patel
Councillor Stephanie Cryan
Councillor Natash Ennin

**Members are summoned to attend this meeting**

**Jeremy Chambers**
**Monitoring Officer**
**Laurence House**
**Catford Road**
**London SE6 4RU**
**Date: 18 November 2024**

The public are welcome to attend our committee meetings, however occasionally committees may have to consider some business in private.

# ORDER OF BUSINESS – PART 1 AGENDA



The public are welcome to attend our committee meetings, however occasionally committees may have to consider some business in private.

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

**Tuesday 26 November 2024 at 6.00 pm**
Southwark Council, Meeting room G01, 160 Tooley Street, London SE1 2QH

**Please note this is being held as an in person meeting, which will also be open for the press and public to attend. The meeting will not be webcast live.**

## Membership:

**Members**
Councillor Fleur Donnelly-Jackson (London Borough of Brent)
Councillor Mili Patel (London Borough of Brent)
Councillor Brenda Dacres (London Borough of Lewisham)
Councillor Amanda De Ryk (London Borough of Lewisham)
Councillor Stephanie Cryan (London Borough of Southwark)
Councillor Natasha Ennin (London Borough of Southwark)

**For further information contact:** Abby Shinhmar, Governance Officer
0208 937 2078; abby.shinhmar@brent.gov.uk

For electronic copies of minutes and agendas please visit:
Council meetings and decision making | Brent Council

**Notes for Members - Declarations of Interest:**

If a Member is aware they have a Disclosable Pecuniary Interest* in an item of business, they must declare its existence and nature at the start of the meeting or when it becomes apparent and must leave the room without participating in discussion of the item.

If a Member is aware they have a Personal Interest** in an item of business, they must declare its existence and nature at the start of the meeting or when it becomes apparent.

If the Personal Interest is also a Prejudicial Interest (i.e. it affects a financial position or relates to determining of any approval, consent, licence, permission, or registration) then (unless an exception at 14(2) of the Members Code applies), after disclosing the interest to the meeting the Member must leave the room without participating in discussion of the item, except that they may first make representations, answer questions or give evidence relating to the matter, provided that the public are allowed to attend the meeting for those purposes.

***Disclosable Pecuniary Interests:**

(a) **Employment, etc. -** Any employment, office, trade, profession or vocation carried on for profit gain.
(b) **Sponsorship -** Any payment or other financial benefit in respect expenses in carrying out duties as a member, or of election; including from a trade union.
(c) **Contracts -** Any current contract for goods, services or works, between the Councillors or their partner (or a body in which one has a beneficial interest) and the council.
(d) **Land -** Any beneficial interest in land which is within the council's area.
(e) **Licences-** Any licence to occupy land in the council's area for a month or longer.
(f) **Corporate tenancies -** Any tenancy between the council and a body in which the Councillor or their partner have a beneficial interest.
(g) **Securities -** Any beneficial interest in securities of a body which has a place of business or land in the council's area, if the total nominal value of the securities exceeds £25,000 or one hundredth of the total issued share capital of that body or of any one class of its issued share capital.

****Personal Interests:**

The business relates to or affects:

(a) Anybody of which you are a member or in a position of general control or management, and:
- To which you are appointed by the council;
- which exercises functions of a public nature;
- which is directed is to charitable purposes;
- whose principal purposes include the influence of public opinion or policy (including a political party of trade union).

(b) The interests a of a person from whom you have received gifts or hospitality of at least £50 as a member in the municipal year;

or

A decision in relation to that business might reasonably be regarded as affecting, to a greater extent than the majority of other council tax payers, ratepayers or inhabitants of the electoral ward affected by the decision, the well-being or financial position of:

- You yourself;
- a member of your family or your friend or any person with whom you have a close association or any person or body who employs or has appointed any of these or in whom they have a beneficial interest in a class of securities exceeding the nominal value of £25,000, or any firm in which they are a partner, or any company of which they are a director
- any body of a type described in (a) above

# Agenda

Introductions, if appropriate.

| Item | | Page |
|---|---|---|
| 1 | **Appointment of Chair**<br><br>To confirm the appointment of the Chair for the meeting.<br><br>In accordance with Section 10 of the Joint Committee Terms of Reference the Chair should rotate between the appointed members from each Council at each meeting. As this meeting is being hosted by the London Borough of Southark the practice is for the Chair of the meeting to be appointed from the membership of that authority. | |
| 2 | **Apologies for Absence and Clarification of Alternate Members** | |
| 3 | **Declarations of Interest**<br><br>Members are invited to declare at this stage of the meeting, the nature and existence of any relevant disclosable pecuniary or personal interests in the items on this agenda and to specify the item(s) to which they relate. | |
| 4 | **Minutes of the Previous Meeting**<br><br>To approve the minutes of the previous meeting held on Tuesday 19 March 2024 as a correct record. | 1 - 8 |
| 5 | **Provision for Public Participation** | |
| 6 | **Shared Technology Service Update Report**<br><br>This report provides an update on the performance of the Shared ICT Service. | 9 - 90 |
| 7 | **Date of Next Meeting**<br><br>To note the remaining programme of date(s) scheduled for meeting of the Joint Committee during 2023/24, as follows:<br><br>• Tuesday 18 March 2025 at 6pm – to be held online chaired by the London Borough of Lewisham. | |

**8 Any Other Urgent Business**

**9 Exclusion of Press and Public**

To consider the exclusion of the press and public from the remainder of the meeting as the remaining report to be considered contains the following category of exempt information as specified in Paragraph 3, Part 1 Schedule 12A of the Local Government Act 1972, namely:

“Information relating to the financial or business affairs of any particular person (including the authority holding that information)"

**10 Shared Technology Service Cyber Security Update Report** 91 - 94

This report provides an update on the Cyber Security status, threats, and mitigations identified in relation to the Shared Technology Services.

# MINUTES OF THE JOINT COMMITTEE OF THE LONDON BOROUGHS OF BRENT, LEWISHAM AND SOUTHWARK

**Held as an online meeting on Tuesday 19 March 2024 at 6.00 pm**

PRESENT (online): Councillor Mili Patel (Chair) and Councillor Fleur Donnelly Jackson (London Borough of Brent), Councillor Stephanie Cryan and Councillor Natasha Ennin (London Borough of Southwark) & Councillor Amanda De Ryk (London Borough of Lewisham)

Also Present: Councillor Paschaud (London Borough of Lewisham)

1. **Appointment of Chair**

**RESOLVED** that in accordance with Section 10 of the Joint Committee's Terms of Reference, Councillor Mili Patel (as representative of the hosting Authority – London Borough of Brent) be appointed as Chair for the duration of the meeting.

2. **Apologies for Absence and Clarification of Alternate Members**

No apologies were received.

3. **Declarations of Interest**

There were no declarations of interest declared by Members at the meeting.

4. **Minutes of the Previous Meeting**

**RESOLVED** that the minutes of the previous meeting of the Joint Committee of the London Boroughs of Brent, Lewisham and Southwark held on Tuesday 28 November 2023 be approved as a correct record.

5. **Provision for Public Participation**

No deputations or request to speak were submitted by members of the public.

6. **Shared Technology Service Update Report**

Kevin Ginn (Head of Operations of Shared Technology Services) introduced the report to the Joint Committee providing an update on key performance areas in relation to the Shared Technology Service (STS).

Members noted the summary of key performance management indicators for the service across all three Council's, which had been included within the report and in terms of detailed service performance, the Joint Committee were advised of the following:

- In this reporting period, STS had made strong progress in meeting three of the main performance indicators, with significant reductions in the number of open STS operational Hornbill calls, the number of open Operational Aged calls (dating back to 2021) and then a significant improvement in SLA performance for priority 3 incident calls and priority 4 (P4) request calls.

- In the period November 2023 through to February 2024, there were ten P1 incidents related to STS infrastructure, four of which were resolved within SLA.

- P3 incidents were the most common type of incident, as these were generally related to issues experienced by individual users. The target SLA was to resolve 90% of P3 incidents within two working days. 10,051 P3 incidents were logged into STS operational queues by the partner councils (11,299 overall) during this reporting period, with an overall SLA performance of 75% (compared with 66% in the previous reporting period) and the top eight categories for P3 calls detailed in section 4.10 of the report.

- Priority 4 were defined as requests for standard service or catalogue item. The standard SLA was to resolve 80% within 5 working days. In the current reporting period, there had been 10,373 P4 requests logged into STS operational queues, with an overall SLA performance of 83% compared with the previous reporting period figure of 74%.

- Response times to P3 and P4 incidents were recorded as faster than they had ever been before, and STS was remaining within SLA across all three local authorities.

- The on-site service for face-to-face visits by users was now covering standard Business as Usual (BAU) hours of 8am to 6pm, as STS strived to improve the user experience further. This service was being provided at the Councils' main offices at Brent Civic Centre, Lewisham Laurence House and Southwark Tooley Street.

- In terms of users needing face to face support, STS had improved the queuing service by implementing the QMinder system, which provided a controlled queueing and notification mechanism, and this will result in tickets being completed quicker.

- The telephony provider was Risual Ltd and when staff rang the IT Service Desk number, it was answered by operatives from Risual who acted on behalf of the three councils. Members were advised of measures being undertaken to resolve an ongoing issue involving the logging of tickets via Risual on Hornbill which had been designed to provide a more accurate picture of first-touch ticket resolution volumes and was also expected would improve SLA performance for P3 and P4 priority tickets. The integration should be delivered by the end of March 2024.

- Overall, the volumes of calls coming into STS were reducing when compared to previous years, which was demonstrative of the mitigation and work put into

place to reduce the number of issues users were facing with a breakdown on tickets logged provided in section 4.15 of the report.

- The Asset Management System had now been fully implemented across all three councils which was being used to manage the issuing, repairs, returns etc. of laptops to users.

- In terms of service user experience a workshop had been held in October 2023 with all councils focussed on areas for improvement, identifying the challenges and opportunities and working together to find solutions, with further details on the programme being delivered in response included under the continuous improvement section in section 5 of the report. This had included use of increased automation and also the potential to utilise AI enabled solutions.

- The details provided on the Top 10 risks identified for STS and the relevant mitigations in place to address them, as detailed within section 6 of the report.

- The details provided on the STS related audits which had been undertaken across all three authorities during 2023-24 along with progress on delivery of the recommended actions identified and audit plan for 2024-25, as detailed within section 7 of the report.

- The outline provided on the 6-month overview of the STS Technology Roadmap, as detailed within section 8 of the report including the refreshment of all laptops of staff across all three councils, wider area networking and improvement of band width and resilience and better network traffic management and Windows Server upgrade (scheduled to be completed by November 24).

- Updates were also provided in relation to a range of other key projects, as detailed in section 9 of the report including the compute and storage infrastructure replacement, Windows laptop pilot, Wi-Fi and network upgrades. Mobile device migration to O2 and renewal of automated switchboard for the Contact Centre with members noting that there were a total of 75 projects currently in flight.

- In terms of the STS budget this was projected to remain in balance to the end of the financial year.

The Chair thanked Kevin Ginn for his update and commended the Service for the performance outlined. Comments were then invited from Members on the update with the following issues raised:

- In response to further details being sought on the O2 migration Fabio Negro stated that Southwark was fully migrated and it was expected that 95% of Brent would be migrated by end of March 2024 and Lewisham in April 2024.

- In terms of open tickets, confirmation was provided that all those from 2021 had now been closed with progress being made in resolving the outstanding requests from 2022.

- Given reference to the Service Improvement Plan, details were sought as to when this would be shared with the Joint Committee given the increasing reliance on IT systems and costs involved with members keen to explore the associated risks in terms of service delivery and impact on residents should systems be unavailable. In response the Joint Committee was advised that STS were aware of the impact on the wider community when issues were experienced with issues reported being classified under different priorities during triage to ensure fast tracking of those systems identified as key or high priority. In terms of costs and value for money, the London Office of Technology and Innovation (LOTI) had been asked to carry out a financial benchmarking exercise on the provision of IT Services across a sample of local authorities, including the STS, which was in the process of being completed and on which further details could be provided as part of the next update for the Committee.

- Further details were sought regarding performance in relation to P1 incidents given their more significant impact on those Councils and services affected especially in cases involving third party suppliers. In terms of these suppliers members were advised of the measures being taken to ensure third party suppliers were integrated into the resolution process with further details requested for the next meeting on the triage process for calls logged and how these were prioritised to reflect the impact on the wider business and local residents.

- Members advised there were also keen to explore the procurement process being developed for the windows laptop refresh across all 3 partner boroughs with a focus on the procurement methodology and provisions included for securing best value, social value and other key considerations. In response the Joint Committee were advised of the work being undertaken with the procurement teams across all three member authorities to review procurement methods and gain a consensus on the right approach going forward including value for money and added social value with work also undertaken in relation to risk and quality assurance. Given the timescales involved, members were advised that a separate paper would need to be provided (outside of the main meeting) outlining the procurement process developed for the windows laptop refresh across all 3 partner boroughs.

As no further matters were raised, the Joint Committee completed their consideration of the update report. The Chair thanked Fabio Negro for the updates provided and it was **RESOLVED**:

(1) To Note the update provided and actions being taken in relation to the ongoing performance and delivery of the Shared Technology Service, as detailed within the report.

(2) In relation to further actions identified:

(a) Further details to be provided as part of the update for the July Committee on the outcome of the VFM benchmarking assessment being undertaken by LOTI on the provision of IT Services across a sample of local authorities, including the STS.

(b) Further details to be provided within the update for the next Committee on the triage process for calls logged and how these are prioritised to reflect the impact on the wider business and local residents.

(c) A separate paper to be provided for members (in advance of the next Committee) outlining the procurement process developed for the windows laptop refresh across all 3 partner boroughs. Update to include a focus on the procurement methodology and provisions included for securing best value, social value and other key considerations.

7. **Date of Future Meetings**

Members noted the following dates scheduled for future meetings of the Joint Committee during 2024-25 Municipal Year:

- Tuesday 9 July 2024 at 6pm – to be held online chaired by the London Borough of Southwark.

- Tuesday 26 November 2024 at 6pm – to be held online chaired by the London Borough of Lewisham.

- Tuesday 18 March 2025 at 6pm – to be held online chaired by the London Borough of Brent.

8. **Exclusion of Press and Public**

At this stage in proceedings the Chair advised that she intended to move into closed session for the remainder of the meeting in order to consider a separate report for the Joint Committee providing updates on the Cyber Security status, threats, and mitigations in relation to the Shared Technology Services (STS).

Given the commercially sensitive nature of the details contained within the update, the Joint Committee were advised that the report would need to be considered in closed session which would require the Joint Committee to pass a formal resolution excluding the press and public for consideration of the item.

It was therefore **AGREED** that that under Section 100A (4) of the Government Act 1972 the press and public be excluded from the remainder of the meeting for consideration of the following item on the grounds that it would involve the disclosure of exempt information as defined in paragraph 3 (information relating to the financial or business affairs of any particular person, including the authority holding that information) of Part 1 of Schedule 12A of the Act (as amended).

*The live webcast was ended at this stage of the meeting to enable the Joint Committee to move into private session.*

9. **Shared Technology Service Cyber Security Update Report**

Kevin Ginn (Head of Operations of Shared Technology Services) then introduced the update report in relation to Cyber Security status, threats, and mitigations for the Shared Technology Service (STS). In considering the report members noted:

- The outline of events impacting on STS along with an update on current threats and mitigating actions in relation to the following key areas of activity as detailed within section 3-7 of the report:
  - DEFEND – which had involved STS developing the means to defend against evolving cyber threats, respond effectively to incidents, and ensure networks, data and systems were protected and resilient.
  - DETER – which had involved STS detecting, understanding, investigating, and disrupting hostile activities against the service.
  - DEVELOP – which had involved STS developing a coordinated and tailored approach to risks and threats encountered and mitigating against potential vulnerabilities.
  - REACT – which had involved STS in developing sufficient controls to respond to any attacks including the organisational channels and processes required to make efficient decisions further protect data and limit any scope of attack.

- The aim to present the future Cyber Security Strategy 2024-2026 to the Joint Committee for approval at the next meeting.

- The outline of future plans being developed in relation to the STS Cyber Security Strategy, as detailed within section 8 of the report, which had included a project focussed on future laptop design as well as work to develop the plans for implementation of Microsoft's biometric authentication method for logging into devices, work to reduce the amount of open old vulnerabilities and to engage with third parties to onboard a Security Operations Centre.

- To protect against privilege escalation in the cloud and on-premise environment, STS had been working with CrowdStrike on their identity protection tool to understand the risk with accounts and the likelihood of exploit and the process to secure corporate identities.

The Chair thanked Kevin Ginn for his update with additional clarification provided for members in relation to the following issues raised:

- The background and resolution of recent cyber security events impacting on the STS across each borough, including the costs and resources involved in dealing with any incidents.

- The approach being developed towards the use of biometrics as a potential security feature.

As no further matters were raised, the Joint Committee completed their consideration of the update report. The Chair thanked Kevin Ginn and Fabio Negro for the details provided and it was **RESOLVED** to:

(1) note the update and actions being taken as detailed in the report.

(2) To request (in view of the issues highlighted during the meeting) a separate paper to be provided for members of the Joint Committee (in advance of the next meeting) on the approach towards the use of biometrics as a potential security feature on devices to be included within the laptop refresh programme including a focus on risks, mitigations and also opportunities alongside consultation with staff representatives/Trade Unions.

10. **Any Other Urgent Business**

None.

The meeting closed at 7.04 pm

COUNCILLOR MILI PATEL
Chair

This page is intentionally left blank

| | |
|---|---|
| | **Joint Committee of the London Boroughs of Brent, Lewisham and Southwark**<br>26 November 2024 |
| | **Report from the Managing Director of Shared Technology Services** |

# Shared Technology Services Update

| | |
|---|---|
| **Wards Affected:** | N/A |
| **Key or Non-Key Decision:** | N/A |
| **Open or Part/Fully Exempt:**<br>(If exempt, please highlight relevant paragraph of Part 1, Schedule 12A of 1972 Local Government Act) | Open |
| **No. of Appendices:** | Four<br><br>Appendix 1: Briefing note for JC for CrowdStrike incident 2024-07-19<br><br>Appendix 2: Laptop Refresh Project – Procurement process review<br><br>Appendix 3: STS Strategy 2024-26<br><br>Appendix 4: STS Cyber Strategy 2024-26 |
| **Background Papers:** | None |
| **Contact Officer(s):**<br>(Name, Title, Contact Details) | Fabio Negro<br>Managing Director of Shared Technology Services<br>Email: Fabio.Negro@sharedtechnology.services |

## 1 Purpose of the Report

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

## 2 Recommendation(s)

2.1 The Joint Committee is asked to:

- To note the progress taken across the various areas in the detail of the report.

- To note the Briefing note for JC for CrowdStrike incident 2024-07-19, attached as Appendix 1

- To note the Laptop Refresh Project – Procurement process review, attached as Appendix 2

- To approve the STS Strategy 2024-26, attached as Appendix 3

- To approve STS Cyber Strategy 2024-26, attached as Appendix 4

## 3 Summary

3.1 STS are preparing tender documentation for the Service Desk Telephone Support. The intention is to conduct an Open Tender procedure to maximise competition within the market. Market Engagement was completed in early October 2024 and concluded there are several different suppliers on multiple frameworks but not a unified framework. Therefore, to maximise the opportunity for best value and competition, the chosen route is Open Tender. The tender is estimated to go live 25 November 2024.

3.2 Brent, Lewisham and LGA have completed the migration from Vodaphone to O2 for the Mobile Voice and Data contract. The previous contract with Vodaphone has ceased.

3.3 STS have completed the Private Cloud Project all servers due to migrate from the old On-premise VMware environment has moved to the private cloud solution of Nutanix, providing the councils with a more robust and performance-rich infrastructure.

3.4 The Laptop Refresh contract has been awarded to CDW, LGA pilot underway, with Brent following. Southwark is in the process of approving the business case for phase 2 of the laptop refresh project. Lewisham's business case for the laptop refresh project is currently being drafted.

3.5 Microsoft Intune pilots are underway in the LGA, with Brent also following. The Intune Build will allow our laptop management to progress from old, outdated solutions to the modern Office 365 Intune environment, transferring all application deployments, the use of Autopilot which can support us to deploy laptops more efficiently and more importantly starting to move our laptops to Windows 11 to ensure we stay in supported levels.

3.6 STS have successfully completed the contract award for Managed XDR (Managed Security Operations Centre) – Cybersecurity Response Service via G-Cloud RM155.17 framework. This will give the councils further assurance that we have monitoring across the laptops in case of any cyber concerns. Essentially, we have procured a third party to respond on our behalf or assist STS in remediating if a cyber issue is to arise.

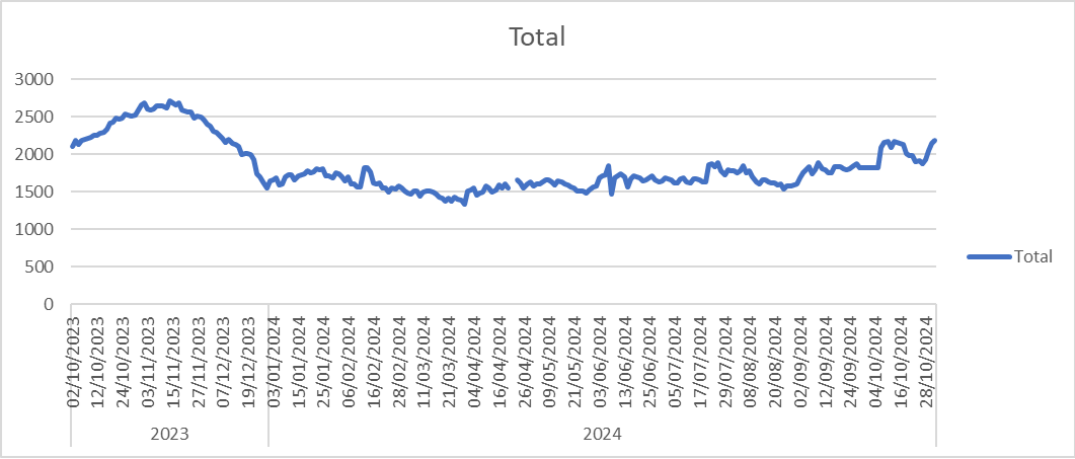
3.7 STS are preparing tender documentation for the Service Desk Telephone Support. The intention is to conduct an Open Tender procedure to maximise competition within the market. Market Engagement was completed in early October 2024, and it concluded there are several different suppliers on multiple frameworks but not a unified framework. Therefore, to maximise the opportunity for best value and competition, the chosen route is Open Tender. The tender is estimated to go live 25 November 2024.

## 4 Service Level Performance

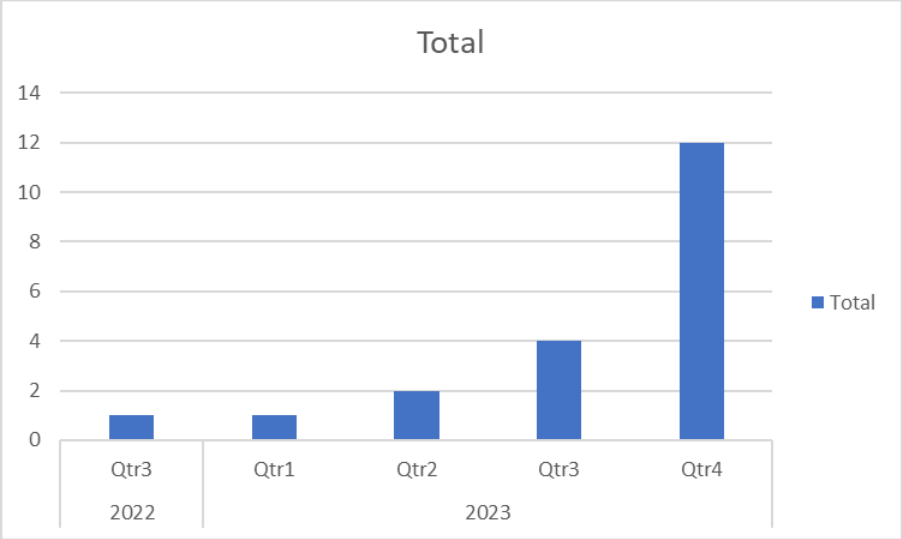
4.1 For the purpose of this report, we have created a section reflecting on Service Levels and broken them down into each of the areas to allow us to provide a better narrative around our performance.

4.2 In this reporting period (July 2024 to October 2024), SLA performance for priority 3 (P3) issues and priority 4 (P4) request calls has dropped slightly compared with the previous reporting period. This is mainly due to a higher level of demand on operational services, such as the mass upgrading of servers (Windows 2012), the rollout of Office 365 applications across the councils, emergency planning, and resilience exercises.

4.3 The chart below shows the number of open calls currently in STS operational queues. We are committed to reducing this number. In October 2023, there were over 2,600 open calls. This figure now stands at around 2,100. There has been an increase in this reporting period, and this is mainly due to a higher level of demand in terms of tickets raised in the STS operational queues. There have been high levels of change across all three councils which has created change-related issues, leading to an increase in incident and request calls.

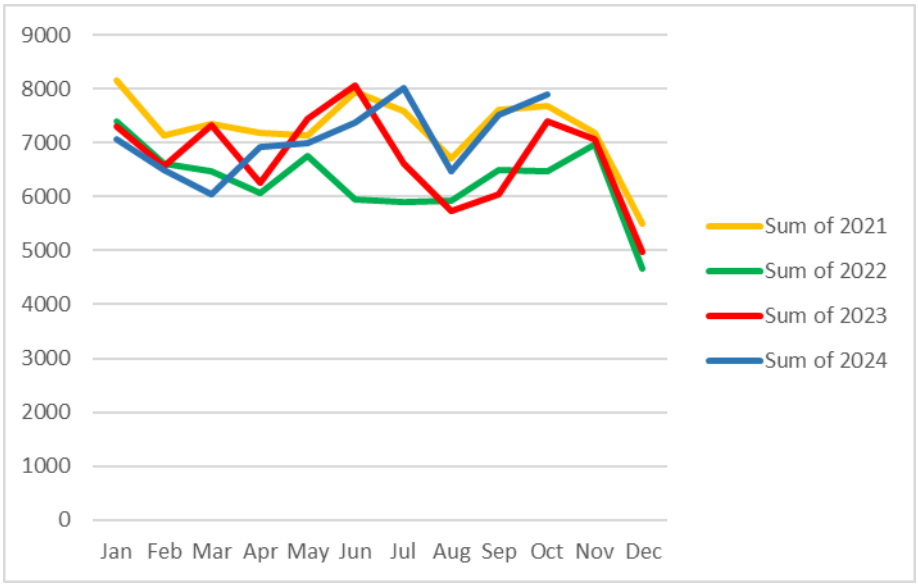



4.4 We continue our drive to close aged tickets in the STS operational queues. The total of open calls raised before 2024 in the operational queues stands at 20 (compared with 43 in the last report), and the chart below shows the date distribution of those calls. Most of the aged tickets from pre-2024 are project-related requests where upgrades are needed. These are reviewed every Friday at the STS Service Delivery Board.




4.5 Since April of this year, we have seen a growing demand on our services with the number of tickets logged into STS queues increasing. Below you will see a graph which identifies the trends of logged tickets into STS queues over the last 3 years and into 2024. It is worth noting that the number of supported users has grown from 10,500 users in 2020 to 12,500 in 2024.

The trend shows that at the beginning of the year, although despite the 15% increase in the user base, we have had fewer calls logged than in previous years, but in the middle part of the year, this has grown in line with previous years. Our aim is to reduce this but it's likely to grow as we start to replace the laptops in the councils as this undoubtedly will raise requests to the service desk.

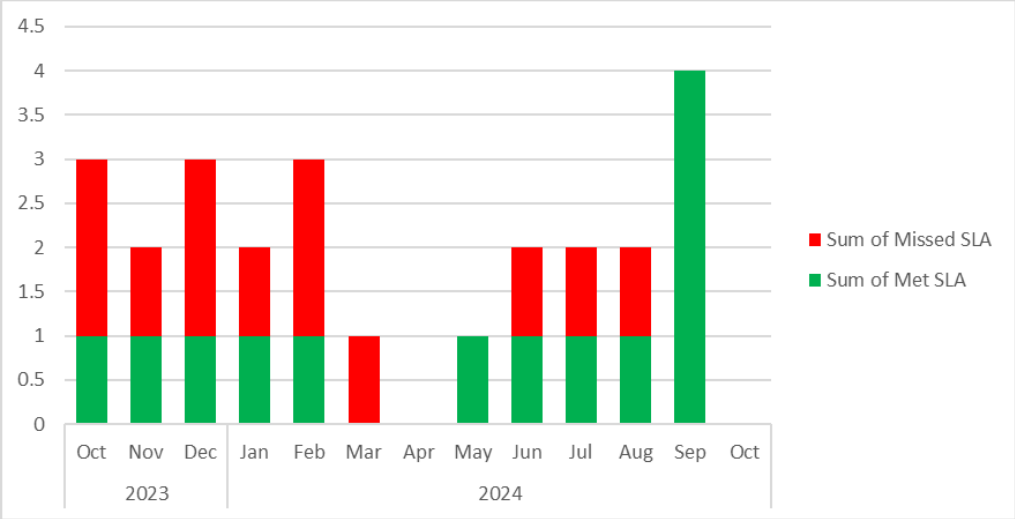



4.6 Priority 1 - Major Incidents

4.6.1 A Priority 1 is classed as a major incident and is defined as an incident that results in the unavailability of or significant degradation to an IT service used by an entire council or councils or the unavailability or significant degradation

of a service impacting upon a whole department, a significant number of users or an entire site or an unavailability or degradation of a critical (Tier 1) business application/service.

4.6.2 In this reporting period (July 2024 to October 2024, there were eight P1 incidents related to STS infrastructure, six of which were resolved within SLA. The below graph shows the number of STS infrastructure-related P1 incidents in the last 13 months.




4.6.3 The SLA target for P1 incidents is three or fewer per month – in the last 12-month period, there were 22 STS infrastructure-related P1 incidents at an average of 1.8 per month, so overall well within the SLA target.

There has been a considerable amount of infrastructure change in that 12-month period, including:

- All three councils replaced the Wi-Fi in the head offices.
- Southwark replaced the network switch infrastructure in Tooley Street.
- New core firewalls have been introduced.
- Migration of mobile phone estate to O2. Brent and Lewisham migrated from Vodafone to O2 and additional controls have been placed around all three councils to avoid toll fraud.
- Due to a Cyber risk, we have replaced the remote access solution for all three councils (from an On-premise Ivanti system to cloud-based Azure App Proxy). The remote access solution is typically used by third parties that support our line of business applications and infrastructure.
- Migration of 4600 Southwark laptops from an old Microsoft solution to F5 VPN for remote connectivity (working away from council offices or when on Wi-Fi within council offices). This has improved the performance for remote working with connecting to the council network and data transfer times being significantly faster.
- Ongoing expansion of Azure cloud services usage.
- OneDrive migrations (Moving users' home folders from on-premise data storage into Microsoft 365 cloud storage).

- Upgrading server operating systems and, in some cases, upgrading applications that may be hosted on those servers.

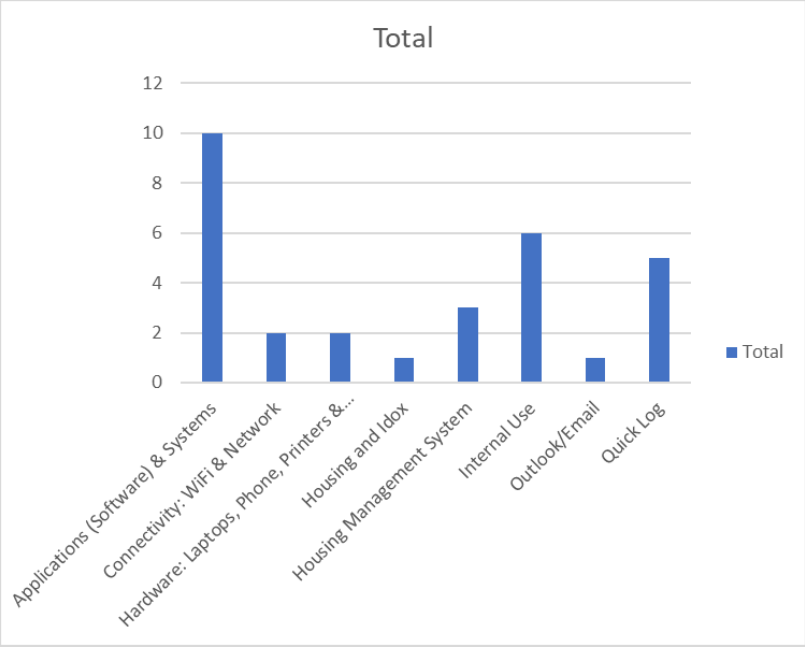
4.6.4 With every major incident that occurs the shared service produces a comprehensive Major Incident Report detailing the impact, timelines, root cause analysis and lessons learned. These reports are distributed to the affected partners and review meetings are held when appropriate or requested.

4.6.5 In this reporting period (July 2024 to October 2024) there were also 6 application/supplier related P1 incidents.

4.7 Priority 2 - Serious Issues

4.7.1 A Priority 2 is a serious issue is defined as an incident that results in either unavailability or degradation of a service which, whilst material, does not meet the threshold for a P1 (Tier 2).

4.7.2 There were 30 P2 calls raised in STS Hornbill operational queues during this reporting period. The target SLA is 30 or less per month – our average for this period is 7.5 per month (compared with 11 for the previous reporting period. The chart below shows the service categories that the P2 incidents were logged against in this reporting period:




4.7.3 The downside is that having so few P2 incidents means that reaching the SLA resolution target of resolving 95% in 8 hours or less can be challenging as only one call failing to meet that 8-hour limit, means the entire monthly SLA fails.

To combat this, we have put in place a mechanism by which as soon as a P2 incident is logged in Hornbill, a notification email will be sent to the STS senior

leadership team members to ensure focus is centred on that incident in a timelier fashion.

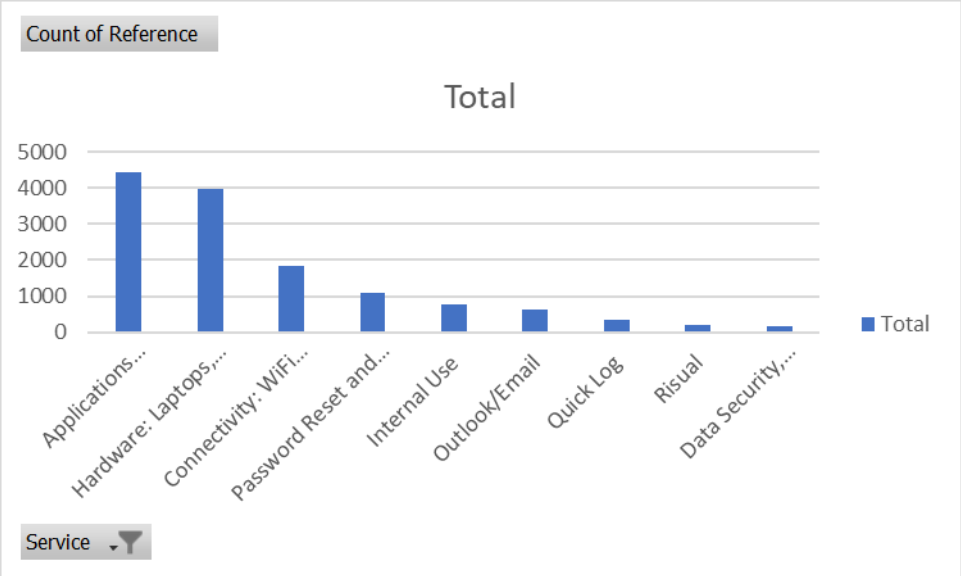
4.8 Priority 3 – General Issues

4.8.1 A Priority 3 issue is defined as one that results in a partial loss of service or functionality with no or limited business impact and for which a workaround may be available.

4.8.2 P3 incidents are far and away the most common type of incident as these will generally relate to issues experienced by individual users. The target SLA is to resolve 90% of P3 incidents within two working days.

4.8.3 13,667 P3 incidents were logged into STS operational queues (14,193 overall into all STS queues) during this reporting period, with an overall SLA performance of 82% (compared with 87% in the previous reporting period). This has coincided with the increase in demand that we have seen in this reporting period. Overall STS has seen around 850 calls more per month logged than in the previous reporting period and the majority of these are P3 incidents. As previously noted, the high-level of infrastructure change is partly responsible for this, but also accompanied by an ageing laptop fleet with failure rates increasing.

4.8.4 The top call raised categories for Priority 3 calls logged in STS Hornbill operational queues during this reporting period are shown below in both chart and table formats:



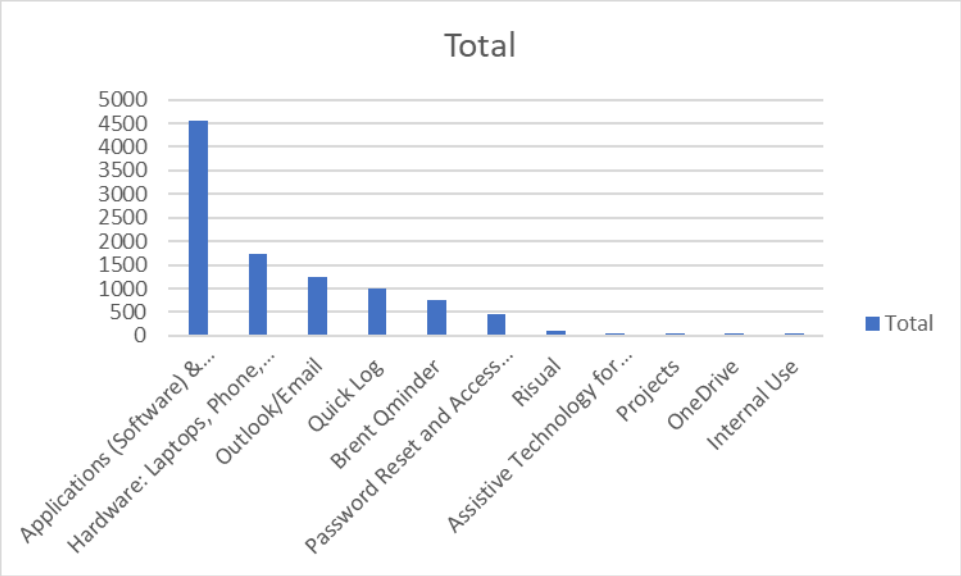
| Call Category | Number of Calls |
|---|---|
| Applications (Software) & Systems | 4416 |
| Hardware: Laptops, Phone, Printers & Monitors | 3971 |
| Connectivity: WiFi & Network | 1852 |
| Password Reset and Access to Shared drives | 1083 |
| Internal Use | 776 |
| Outlook/Email | 647 |
| Quick Log | 344 |
| Risual | 204 |
| Data Security, Phishing, Lost/Stolen items | 170 |

4.9 Priority 4 - Service Requests

4.9.1 A Priority 4 request is defined as a request for standard service or catalogue item. The standard SLA is to resolve 80% within 5 working days (although SLA can be negotiated with the user logging the call depending on the nature of the request e.g. a request for a new network link to a site to be installed – this can take several months).

4.9.2 More typical requests are for applications to be installed onto a laptop, or a request for new kit such as a mobile phone.

4.9.3 In this reporting period there were 10,137 P4 requests logged into STS operational queues (10,635 logged into all STS Queues), with an overall SLA performance of 90% compared with the previous reporting period figure of 93%. The SLA performance has dropped slightly, and this has been impacted by the increased number of P3 incidents as previously noted, with incidents having a higher priority level than requests. The chart and table below show the top call logging categories for STS operational P4 requests.



| Call Category | Number of calls |
|---|---|
| Applications (Software) & Systems | 4560 |
| Hardware: Laptops, Phone, Printers & Monitors | 1731 |
| Outlook/Email | 1249 |
| Quick Log | 1001 |
| Brent Qminder | 762 |
| Password Reset and Access to Shared drives | 467 |
| Risual | 108 |
| Assistive Technology for Specific Accessibility Needs | 56 |
| Projects | 56 |
| OneDrive | 43 |
| Internal Use | 38 |

4.10 Onsite support

4.10.1 The onsite teams across the three partner councils typically take care of three major functions:

- Local on-site support in the main partner offices (Brent Civic, Lewisham Laurence House and Southwark Tooley Street).
- Non-main office site support. Between them the three councils have around 230 office sites that STS manages network links to.
- Starters, Movers and Leavers (SMaL) acceptance and processing.

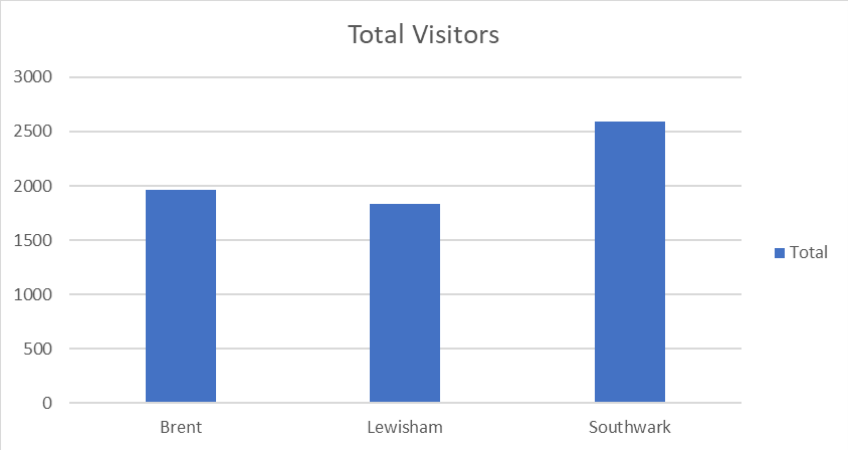
4.10.2 The on-site service for face-to-face visits by users is now covering standard BAU hours of 08:00 to 18:00 without any break as we strive to improve the user experience further. This service is provided at the Councils' main offices of Brent Civic Centre, Lewisham Laurence House and Southwark Tooley Street.

4.10.3 The QMinder system allows us to provide a controlled queueing and notification mechanism for those users needing face-to-face support. The statistics for this reporting period (July 2024 to October 2024) produced by QMinder show that across the three main partner locations:

- There were 6,382 visits (compared with 6,134 in the previous reporting period) – the graph below shows visitor distribution by location. This growth in demand is inline with that we have seen across the rest of the operational service. But we have been able to maintain service at similar levels to the last reporting period in terms of wait and service time. The table below shows the top reasons for onsite visits.

| Issue | Visitors |
|---|---|
| Laptop/iPhone Hardware Repairs | 2199 |
| Laptop/iPhone Collect -Starter | 829 |
| Wi-Fi/Network Issues | 823 |
| Applications | 787 |
| New Starters/Leavers/Movers | 392 |
| IT Accessories | 305 |
| Password Reset | 296 |
| Laptop/iPhone Return - Leaver | 124 |
| Password/Account Locked issues | 114 |
| Hardware | 72 |
| Broken Laptop/ phone | 39 |
| **Grand Total** | **5980** |

- Across all sites, an average wait time of 27 minutes (compared with 26 minutes in the previous reporting period).
- Across all sites, an average service time of 35 minutes (compared with 29 minutes in the previous reporting period).

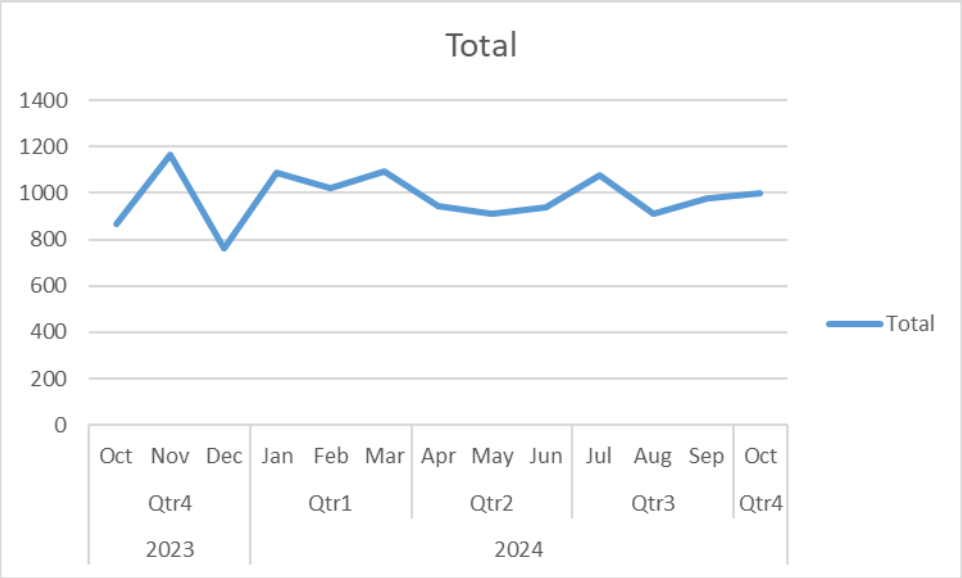



4.11 Telephony Support

4.11.1 Node4 (formerly Risual) are our telephone service provider for our IT Helpdesk. When staff ring the IT Service Desk number, it is answered by engineers from Node4, who act on behalf of the three councils. We have given them the access permissions to be able to resolve tickets on our behalf. We have also provided them with the scripts needed to understand our configuration although more work is needed to encourage higher first-time fix rates.

4.11.2 The contract with Node4 was renewed in April and part of that was to negotiate a formal SLA for telephone answering times to address concerns previously raised around call wait times. The SLA agreed is that 80% of calls should be answered within 5 minutes (penalties in the form of service credits will apply should this target not be met).

4.11.3 We have engaged with Node4 to add an integration that allows Node4 to carry on logging tickets into their Microsoft Dynamics ITSM tool, but this will then use an API to automatically log a ticket into our Hornbill system. This will allow us to have a clearer picture of how many calls are being logged and resolved by Node4. This integration was completed in this reporting period. The table below shows the volume of tickets logged by Node4.




4.12 User Experience

4.12.1 Due to an issue with the NPS reporting mechanism we are unable to report on the Net Promotor Score (NPS) survey score for this reporting period. (When a Hornbill call is resolved, the user that logged the call has an opportunity to complete a brief survey about the call resolution experience – the overall NPS score is calculated from the results of the survey and reflects our colleagues' level of satisfaction with the service provided. Anything around 60% is regarded within the industry as excellent).

4.12.2 The Net Promoter Score measures are now seen as a measure of loyalty that customers have towards an organisation and its services, hence NPS surveys nearly always include a question that asks whether the customer would recommend the service to friends and family members. This approach is not appropriate any longer for STS as our colleagues have no choice in using our services. Instead, we are developing a survey using a customer satisfaction measurement (CSAT) instead. This should be released very shortly.

4.13 Overall Call Number Statistics

4.13.1 The shared service logged 57,889 tickets between July 2024 and October 2024 for all council application teams as well as the shared service (an average of 14,472 tickets per month) against 53,147 in the last reporting period, March 2024 to June 2024 (an average of 13,287 tickets per month). These tickets consisted of both incidents and service requests. This

total is broken down by (previous reporting period numbers in parentheses).

- Shared Technology Services – 29,965 - an average of 7,491 per month (previous reporting period March 2024 to June 2024 – 26,557 - an average of 6,639 per month).
- Brent Applications Teams – 18,208 - an average of 4,552 per month, previous reporting period March 2024 to June 2024 – 16,766 - an average of 4,192 per month).
- Lewisham Applications Teams – 4,427 - an average of 1,107 per month, previous reporting period March 2024 to June 2024 – 4,451 - an average of 1,113 per month).
- Southwark Application Teams – 5,127 - an average of 1,282 per month, (previous reporting period March 2024 to June 2024 – 5,177 - an average of 1,294 per month).
- LGA Internal support – 162 – an average of 41 per month (previous reporting period March 2024 to June 2024 – 90 – an average of 22.5 per month).

4.14 Service Improvements

4.14.1 While the last 12 months has seen an improvement in performance against key SLA KPIs, in addition, we are now looking at how we can improve the customer experience. Some of the key actions around this are:

- We are currently trialling (in one of the councils) a new on-site approach for visitors. We have removed the requirement for visitors to the on-site to log Hornbill calls prior to the visit. Our engineers will log calls on their behalf.
- We have introduced new signage in the form of a roller banner at the registration desk to guide users through the process of registering with the QMinder System
- We have also used the banner to publicise a QR Code/URL that users can access from their mobile devices to check how busy the onsite team is (how many visitors are in the queue) and what the average wait time is.
- We have also introduced a scripted welcome for our engineers to follow to provide a more welcoming and consistent experience for visitors.

We will be rolling this out to all partners in the very near future.

4.14.2 As well as the current improvements, we are also looking to the future and we will be introducing a reception/concierge service to greet colleagues when they visit the on-site team. This will provide a rapid triage service to ensure we understand the nature of the issue and so hopefully can resolve faster. It will also allow us to provide a very quick service for those visitors that have attended but do not need to see an engineer e.g. they may be there just to pick up something simple like a laptop bag or a spare set of headphones.

4.14.3 We will also be looking at how we can improve the induction process for new starters. One idea is to ensure this happens at the same time as an HR induction to provide a better and one-time experience for new staff members.

4.14.4 Our Service Desk Telephone Support Line Service contract is due for renewal on the 1 April 2025. One of the service-improvement options that will be in the tender will be for a comprehensive IVR system that will provide features such as:

- Customised messages in the event we need to notify callers of any major incident that may be affecting service.
- Self-help options for common issues such as using self-service password reset.
- Giving an expected wait time to be connected to an engineer and a position in the queue.

4.15 Hornbill Call Management

4.15.1 Hornbill call triage. We have also looked at improving our call triage times. Triaging a newly logged ticket involves:

- Ensuring the call has been logged under the correct type i.e. Incident or Request as this determines the automatically assigned priority which in turn defines the call resolution SLA.
- Checking sufficient information about the issue or request has been given and if not update the call asking the user to provide the necessary details.
- Assigning the call to the correct team for further investigation and resolution.

While there is no specifically defined call triage SLA or KPI, STS aims to assign calls to teams within 20 minutes of submission. Triaging has been improved dramatically by using workflows within Hornbill to assign calls automatically to the correct resolver team, where any further manual triaging can be carried out. This has also had a positive impact on our overall SLA performance.

4.15.2 Hornbill Call Escalation. We have refined the Hornbill call escalation process for users to be able contact us about the progress or management of a ticket they have raised with us. It should be noted that escalations should only be used if the call resolution time SLA has been, or is close to being breached, or if it is believed that a call has been given the wrong priority level. There are 4 stages of escalation:

1. Contact the engineers assigned to the call via the Hornbill portal or call the engineer directly.
2. Email the IT escalation mailbox. This mailbox is monitored by a team leader who will investigate and aim to resolve your incident, request or complaint.
3. Email the STS Service Desk Manager.
4. Email STS Head of Operations & Service Desk Manager

Complaints can also be directed to the STS Head of Operations. In addition, we also have a VIP category of users within Hornbill. This category is limited to those users who have critical functions within the council and may require calls to be expedited to avoid a negative impact on the business. The triage queue is monitored for VIP calls and then assigned immediately to an engineer who is also informed of the newly raised call.

## 5 Continuous Service Improvement

5.1 The team has focused improvement initiatives focusing on main streams such as User Experience, Assets, SMaL process. Below is a flavour of what they have worked on in the last 3 months, including:

- Ongoing Hornbill redesign, including updating the User Interface and improving the capture forms by making tickets easier and quicker to log, whilst capturing the correct information.
- Reporting Trends Database, including data going back to Jan ’23. With this we can set baselines and analyse common trends.
- Dynamics – Hornbill integration, which removes the need for Risual/Node4 agents to double log and ensures we capture all reporting of First Time Fixes.
- InTune – Hornbill connection fully established with all orgs having mobile & tablet data within the Asset Management System.

5.2 Our short-medium term plan is focused on the areas below, but there are other areas such as the laptop refresh, the Telephony tender and SMaL processes across the orgs that will be supported by the Service Improvement Team. Long-term we will look at our ITSM and whether replacing it will be the optimal strategic plan.

5.3 We are close to finalising our restructuring of the STS teams, with the aim of increasing the members of staff on the frontline to accommodate each councils needs.

5.4 We have also commenced market research on IT Service Management solutions, initially to understand what the ‘art of the possible’’ is.

| Item | Update | ETA |
|---|---|---|
| NPS/CSAT Improvement – Phase 1: New form and reporting | Setting up new CSAT form with better UX and reporting capabilities, with automated workflow | Dec-24 |
| LBB Oracle – Hornbill integration | Soft launch to go live soon, with fully go live date in December | Dec-24 |
| Hornbill 3.0 – Phase 1: UX | Continuously iterating and launching new flows, ongoing improvements | Jan-25 |
| Automated Asset Power BI | Iteration on current Asset Database, using Power Automate to have daily updates – improve focus on data gaps | Feb-25 |
| Hornbill 3.0 – Phase 2: Service Specific Support / Closure Codes | Improving customer journeys for all service areas / improving closure codes for incident logging to enable better Problem Management Process | Mar-25 |

| | | |
|---|---|---|
| NPS/CSAT Improvement – Phase 2: Close feedback loop | Send automated follow ups to responders and engage with them for specific feedback to ensure issues are addressed | Mar-25 |
| Hornbill 3.0 – Phase 3: Knowledge Base / Automations | Establish use of new Knowledge Base feature for wider use / work on automated processes to reduce repetitive tasks for engineers | Jun-25 |
| Hornbill AI possibility | Understand possibilities of initiating Hornbill AI features using locally hosted Azure servers | ? |

5.5 The entire service has been attending Equality, Diversity and Inclusion Training, the training is being facilitated by an external specialist and has been received well, the schedule is due to complete this summer.

## 6 Risks

6.1 Our STS risk register is reviewed monthly by the Senior Leadership Team and uses Microsoft “Lists” so that it is available to all senior IT management in the partner Councils.

6.2 These are the Top risks identified for STS currently:

| Category | Description | Current Probability | Current Impact | Current Risk | Target Risk |
|---|---|---|---|---|---|
| Security | Cyber Security (DDoS/virus/malware/hacking) resulting in complete loss of user access to all systems, or complete system failure, requiring manual operation to continue business | 5 | 5 | 25 | 15 |
| Financial | Uncontrolled spend on Azure services affecting budgets of partners | 5 | 4 | 20 | 8 |
| Security | There is a heightened risk of a Cyber attack from Russia due to the war in Ukraine and the subsequent UK response of sanctions and support. Other conflicts around the world are also a potential indirect threat. | 4 | 5 | 20 | 16 |
| Financial | Savings Targets for 2025-26 onwards may put at risk our ability to meet our service levels | 5 | 3 | 15 | 0 |
| Financial | Too much reliance on one vendor for a large part of our required services could result in lower ability to control costs | 3 | 5 | 15 | 15 |
| Security | Incomplete Inventory of Software Assets | 5 | 3 | 15 | 6 |
| Security | Increasing threat of data loss via our IT supply chain, including business applications. | 5 | 3 | 15 | 10 |
| Security | No Network based intrusion detection and / or prevention. | 3 | 5 | 15 | 10 |
| Security | Unauthorised External access to Council systems resulting in either denial of service and or loss/compromise of Council data that may prevent business operations form running and impact Citizens directly | 3 | 5 | 15 | 10 |
| Technical | Applications, Hardware and Systems becoming end of life or out of support creating security and operational. | 5 | 3 | 15 | 9 |
| HR | Unable to recruit/retain/afford sufficient skilled and qualified staff to run the service.<br>Unable to deliver project work at rate required by the business<br>Pressure to reallocate “business a usual” resource onto projects | 3 | 4 | 12 | 8 |
| Performance | No User Experience monitoring | 4 | 3 | 12 | 12 |
| Security | Ransomware Affects whole infrastructure including backups. | 3 | 4 | 12 | 12 |

6.3 As part of STS’s ongoing initiative to strengthen our partner’s Cyber awareness, a number of Emergency planning Cyber Exercises Lessons have been held in the past year.

In Brent, following a successful exercise in March, a second exercise was conducted on July 23rd for Gold and Silver command-level participants, and a third exercise focused on Adult Social Care and Children and Young People services was completed on August 20th.

Three exercises have been successfully carried out in Lewisham over the past year, with the next exercise planned for January or February 2025.

Southwark's exercise on July 31st was well-received and underscored the need for business areas to enhance both business continuity and contingency plans.

Additionally, the Emergency Planning (EP) Cyber Exercises Lessons Learned workshop was conducted successfully. It was agreed that these workshops would be held quarterly, and a Teams channel has been established to facilitate efficient resource and outcome sharing among STS and partner organisations.

## 7 Audits

7.1 The last period has seen the following audits progress:

- Southwark Hardware Asset Management – Final report issued and a rating of "Moderate" for Control Design and "Limited" for Control Effectiveness. Three actions were recommended from this report, two of which have since been implemented with the final action progressing on schedule.
- Southwark Service Review - Final report issued and a rating of "Substantial" for Control Design and "Moderate" for Control Effectiveness. Two actions were recommended from this report, both have been implemented.
- Southwark Incident Management Review – Final report issued and a rating of "Substantial" achieved. No actions have resulted from this report.
- Southwark Cyber Security Review – Final report issued and a rating of "Moderate" for Control Design and "Limited" for Control Effectiveness. STS had three recommendations, two of which have since been implemented, with the third awaiting change approval before implementing. To progress all the recommendations in this report, a weekly meeting now takes place with Southwark and STS representatives to work through the action plan.
- Southwark Financial Management Review – awaiting the draft report.
- Brent Project Management Review – Terms of Reference have been agreed, and the audit is scheduled for January 2025.
- Brent Project Management Review – Terms of Reference have been agreed, and the audit is scheduled for January 2025.
- Brent IT Procurement Review – Terms of Reference have been agreed, and the audit is scheduled for November 2024.

7.2 The plan for FY24/25 audits was discussed on 18th March 2024 and is currently as follows:

| # | Council | Proposed Audit Title | Outline description / reasoning | Proposed Timing | Circulated? | Status | Q1 | Q2 | Q3 | Q4 |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Lewisham | IT Support (not completed 23/24) | Assurance rated work on effectiveness of IT support in resolving user-reported issues. | Q1 | No report | Closed | | | | |
| 2 | Southwark | Financial Management | Monthly reporting, accuracy, timelines | Q3 | | Underway | | | | |
| 3 | Brent | Procurement | Review of procurement governance | Q3 | | Underway | | | | |
| 4 | Southwark | Incident Management | Across LBS and shadow teams | Q3 | | Closed | | | | |
| 5 | Southwark | Change Management | Across LBS and shadow teams | Q3 | | Underway | | | | |
| 6 | Lewisham | IT Application Security | | Q3 | | Underway | | | | |
| 7 | Brent | Project Management | Focus on STS PM processes, controls and reporting | Q4 | | Underway | | | | |
| 8 | Southwark | Cyber 3rd Party Supply Chain | Including LBS Supply Chain | Q4 | | Planned | | | | |
| 9 | Brent | SLAM Process (not completed 23/24) | Following new Asset Management & Oracle development (Delayed), review of the SLAM processes and controls | | | To Schedule | | | | |
| 10 | Brent | IT Application | Business line application (DB to propose) | | | To Schedule | | | | |
| 11 | Brent | Performance and Availability monitoring | Scope to be confirmed with DB/MK/MG | | | To Schedule | | | | |
| 12 | Lewisham | Starters and Leavers (not completed 23/24) | Wider LBL audit, with input from STS | | | To Schedule | | | | |

7.3 Recommendation Actions progress summary is below:

**Open Audit Actions**

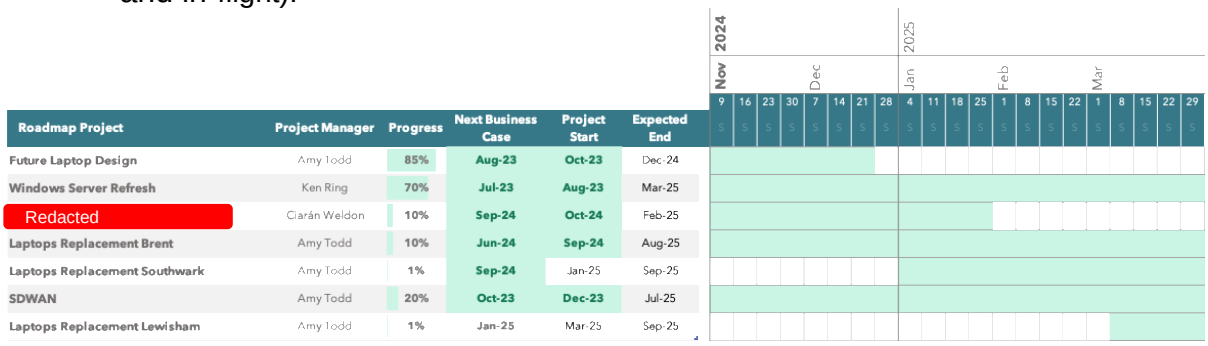
| Partner | High | Low | Medium | Total |
|---|---|---|---|---|
| ⊟ Brent | | | | |
| 3rd Party Supply Chain | | | 1 | **1** |
| ⊟ Southwark | | | | |
| Cyber Security | | 1 | | **1** |
| IT Asset Management | 1 | | | **1** |

7.4 Since the last report, 16 audit recommendations have been completed. In total, we currently have 3 recommendations where actions are underway:

| Partner | Audit | Task Name | Priority |
|---|---|---|---|
| Brent | 3rd Party Supply Chain | Ref 7 - Redacted | Medium |
| Southwark | IT Asset Management | Ref 1 - Disposal / Data Destruction process | High |
| Southwark | IT Cyber Security | Ref 8 - Redacted | Low |

## 8 Technology Road Map 2026 and Forward Plan

8.1 Below is the next 6-month view of our Technology Roadmap Projects (planned and in-flight):



| Roadmap Project | Project Manager | Progress | Next Business Case | Project Start | Expected End |
|---|---|---|---|---|---|
| Future Laptop Design | Amy Todd | 85% | Aug-23 | Oct-23 | Dec-24 |
| Windows Server Refresh | Ken Ring | 70% | Jul-23 | Aug-23 | Mar-25 |
| Redacted | Ciarán Weldon | 10% | Sep-24 | Oct-24 | Feb-25 |
| Laptops Replacement Brent | Amy Todd | 10% | Jun-24 | Sep-24 | Aug-25 |
| Laptops Replacement Southwark | Amy Todd | 1% | Sep-24 | Jan-25 | Sep-25 |
| SDWAN | Amy Todd | 20% | Oct-23 | Dec-23 | Jul-25 |
| Laptops Replacement Lewisham | Amy Todd | 1% | Jan-25 | Mar-25 | Sep-25 |

8.2 We are now in the 4th year of our current 5-year investment plan with the majority of the infrastructure transformation having been delivered. Over the next calendar year, we will upgrade all laptops to Windows 11 or, if the laptops are end of their useful life, replace them.

8.3 A future IT Modernisation investment plan is now being formulated for 2026-2030. We are planning joint workshops with partner councils to develop the

strategy for this new plan. It is expected that the new plan will be presented to Joint Committee in the first half of next year.

## 9 Project Updates

9.1 Future Laptop Windows 11

Microsoft will end support for Windows 10 in October 2025. This project is part of STS transition strategy to ensure all systems and operations continue without interruptions or security risks linked to unsupported software and hardware.

9.1.1 The hardware tender for providing Lenovo devices to LGA and Brent has been awarded to CDW. We are currently in discussions with CDW to finalise the service agreement for managing repairs and delivering new laptops to staff, the ambition is to elevate the level of cover we have to ensure a better turn around for staff who have issues with the laptop.

9.1.2 We have tendered for the Microsoft Intune setup, and Softcat has been awarded the contract. “Make IT Happen,” a subcontractor to Softcat, is responsible for its delivery. The LGA Microsoft Intune tenancy setup is currently undergoing testing during the laptop pilot phase. We will have started development on all three councils' environments.

9.2 Laptop Always On VPN

The council's remote working system, Microsoft Direct Access, was useful during the pandemic; however, it experienced speed and connection limitations. Additionally, Microsoft has announced that it will no longer develop this product. Consequently, a new solution, AlwaysOn VPN, has been introduced to provide seamless connectivity to all Microsoft services. This replacement addresses the existing limitations and aligns with Microsoft's future development direction, ensuring optimised performance and enhanced connectivity for the council's remote workforce.

9.2.1 Southwark's AlwaysOn VPN deployment was completed successfully in November 2023.

9.2.2 The deployment of AlwaysOn VPN is currently underway at LGA. At LGA, user acceptance testing is being conducted on new laptops that are part of the laptop refresh project pilot.

Brent has deployed AlwaysOn VPN to a small group of users for testing. Upon successful completion of the testing phase, the pilot will conclude and AlwaysOn will be rolled out to laptops as part of the laptop refresh project pilot.

9.2.3 AlwaysOn VPN has been deployed to a larger pilot group in Lewisham, who have indicated that they will maintain most of the existing laptop inventory when upgrading to Windows 11 as part of the laptop refresh project.

9.2.4 VPN is a module of a wider group of security tools, Southwark have expressed their interest in Zero Trust Security, which we are exploring collectively, we are currently reviewing the marketplace for suitability.

9.3 Network Upgrades

The proposed solution involves implementing SD-WAN technology to replace the current dedicated leased line site-to-site circuits. SD-WAN offers the advantage of utilising internet connections instead, providing significantly enhanced flexibility in routing network traffic. For instance, traffic related to Microsoft 365 applications such as MSTeams and email can be directed straight from the site to Microsoft servers, bypassing the need to route through the council data centres. This upgrade promises to optimise network efficiency and improve overall connectivity for the councils' operations.

9.3.1 Brent has 34 sites within the scope, and STS has completed surveys for 27 of these sites. Virgin Media has conducted 3 site surveys to date, with an additional 3 surveys scheduled.

9.3.2 Lewisham has confirmed that 33 sites are within the scope. To date, STS has completed surveys at 24 of these sites, and Virgin Media has completed surveys at 4 of them.

There remain a few stages to be completed before these 4 sites will be SDWAN ready.

9.3.3 As part of phase 1 of the Southwark rollout, 87 sites are now in flight. Of these 87 sites 18 can be completed with 15 ready for migration.

9.4 Windows 2012 Upgrades

All councils operate multiple Windows 2012 servers, with their support stated to end in October 2023. It is crucial that we prioritise upgrading these systems. Additionally, for services expected to continue beyond October 2023, we have procured additional licenses to ensure extended support. This is imperative to ensure that we continue to get updates to protect us from any cyber threats.

9.4.1 As of October 31, 2024, the Brent server estate originally comprising 218 servers running Windows Server 2012, has seen 198 servers either decommissioned or in the process of being decommissioned. Of the remaining 20 servers, all are currently undergoing this process, with the majority expected to be completed within the next few weeks. However, some servers hosting applications and services will require additional time for resolution. The Project Manager will submit a change request to seek approval for re-baselining the completion date, now anticipated to be by the end of 2024.

9.4.2 As of October 31, 2024, 204 servers were running Windows Server 2012 in the Lewisham server estate. Nine were out of scope. Of the remaining 195 servers, 172 had been or were being decommissioned. Remediation for the

final 23 servers is discussed in weekly status reviews. A change request will be raised to extend the completion date to January 2025.

9.4.3 Of the 87 Southwark Windows 2012 servers identified for STS migration, 30 were out of scope. By October 31, 2024, 51 had been decommissioned. Of the remaining 6 servers, 3 require third-party action, and the other 3 are awaiting signoff on replacement servers before decommissioning can proceed.

9.4.4 LGA had 40 servers in scope and as of 31st October 2024 39 had been completed. The final server is in the process of being decommissioned.

9.4.5 Lewisham Homes Windows 2012 servers that need to be is being treated as a separate project. 89 Servers have been identified with 44 being decommissioned.

9.5 Telephony and Contact Centre

9.5.1 For Brent and Lewisham, the Telephony the intention is to renew with 8x8 by compliant framework route. This is based on the rationale to avoid disruption to service and the cost of transition from an incumbent supplier to a new vendor. Southwark are intending to award to a new Vendor. The management of back-office telephony will be undertaken by STS as part of our infrastructure services. This system is designed to integrate seamlessly with any telephony products that the Council decides to implement. As all services are cloud-hosted, there will be no need for additional infrastructure changes related to back-office telephony.

## 10 Procurement Updates

10.1 STS has appointed a new Commercial Procurement and Contracts Manager, who has a wealth of experience started on the 16th of August 2024.

10.2 The tender for Microsoft Intune (Device Management) is completed and the contract has been awarded to Softcat.

10.3 The tender for provision of laptops has been completed for both Brent and LGA. The contract was awarded to CDW. In August 2024 for 4,500 Lenovo devices. These will be deployed across both organisations starting from November 2024.

10.4 The Procurement for Adobe Licences for Southwark is completed, and contract start date is the 6th of July 2024. The renewal for Brent is due March 2025, and Lewisham is due December 2024.

10.5 SDWAN - The network circuit requirements are sourced through contract with the London Grid for Learning (LGfL) for Brent and Lewisham. Contract was awarded to LGfL in January 2024 and the rollout of Virgin Media Circuits with an SDWAN overlay is underway in all three Boroughs.

10.6 STS have extended Ricoh UK Limited: Printing Services - extended by 12 months. Two further 12-month permissible extensions are available as part of the existing contract.

10.7 STS Service Desk Telephone Support – Market Engagement was completed during October 2024, there are a variety of suppliers in the market offering competitive pricing. STS are underway with drafting tender documents for open procedure based on the needs of all three Boroughs.

The tender will be under one Lot devised of two Options on a 'Bronze' and 'Silver' level of requirement. Bidders will be required to submit tender responses or both Options and provide additional bolt-on costs for information purposes. These bolt-ons will be included in the price schedules and can be added as additional requirements throughout the term of the contract independently by the Boroughs. The recommended route to market has been identified as most economically advantageous solution.

10.8 Microsoft Licences

Microsoft licenses for Brent, Lewisham and Southwark have been renewed. Southwark's new contract has commenced under preferential discounted pricing for UK Public Sector. All STS Microsoft contracts are renewed/awarded under Digital Transformation Arrangement21 (DTA21) which comes with 33% discount offer on all Microsoft products.

10.9 Telecoms Expense Management Service – The existing service with Nuvoli is part of a variation to the overarching Mobile Voice and Data Contract with VMO2. The service is due to end in December 2024, and negotiations with the supplier are underway to secure a saving.

10.10 We are also exploring with another billing monitoring supplier who are running a savings exercise free of charge to see if there are any more savings to be gained. This will provide Partners and STS an assurance that we are getting best value or provide us with options to make more savings in the future.

## 11 Council Updates

11.1 Brent Digital Update

11.1.1 Brent's digital programme began in 2017 when our first digital strategy was agreed. Cabinet agreed a refreshed Digital Strategy for 2022-26 in December 2021. As part of the delivery of the digital strategy for 2022-26 several projects of work have been delivered within 2024-25. This includes system upgrades, migrations to new software, digital inclusion support for residents and deployment of new apps for residents. Examples of projects delivery in 2024 include:

- Exceeded 2026 connectivity target of 62% (currently 71%)
- Updated My Account – improving residents experience and support channel shift with over 202,400 currently registered. This includes the

implementation of e-shot technology providing automation and real-time data synchronisation will lead to increased efficiency in managing all the email subscriptions. Additionally, First Wave Housing and I4B services were added to My Account, reducing telephone calls, improving resident experience and supporting revenue generation.

- At the end of Q4 for 23/24, calls were reduced from 677,173 in 2022 to 400,121 which is a reduction of 41% in calls.
- M365 has been rolled out across the organisation, providing improved collaboration and security.
- All home drives have been migrated to OneDrive, supporting improved use of M365 and opportunities for collaboration.
- Document storage review was completed consolidating various paper document storage contracts and digitising where appropriate.
- Updates and remediation have been made to Dynamics including housing block audits, tenancy audits, patch allocations and dashboards.
- Over 200 digital champions have been recruited to support residents with developing digital skills.
- Over 3,000 devices have been provided to digitally excluded residents via the Digital Support Fund for Children and Young People and Resident Digital Support Fund
- 33 processes have been automated with RPA (Robotic Process Automation) providing operational efficiency by automating repetitive tasks, reducing errors and freeing up staff time to focus on value-based activities within the business process. These RPAs have been deployed across customer access, council tax, debt recovery, adult social care and school admissions. An average of £30,000 has been realised with each automation
- Four chatbots have gone live reducing calls and supporting channel shift and improving customer experience. An average of 1200 enquires are resolved via the chatbot. This includes a library chatbot, enabling residents to find out information about local community groups and provisions
- Soft market testing and engagement with Children and Young People and Adult social care has identified Mosaic on Cloud as a the most appropriate case management solution.
- A trial of CoPilot took place to ensure security and infrastructure compliance. Use cases will be identified for further roll out of the pilot.
- 21 community buildings have been connected with full fibre to the premises via grant funding
- Mealia App which helps residents with their planning, shopping and cooking of their meals based on their budget, dietary requirements, kitchen equipment etc. has been deployed
- Temporary Accommodation calculator phase 2 was complete which includes additional functionality such as license agreements, task assignment to housing benefit officers, and docusign functionality.
- We have hosted a Brent Digital Day for all staff to promote existing technology across the council and commence a digital skills development programme

11.2 Lewisham Digital update

11.2.1 The Digital Product & Development team has outlined key objectives for 2024-25 focused on revenue growth, cost reduction, and improved satisfaction for residents and employees. They aim to enhance the user experience by tracking satisfaction through data sources like Hotjar, Microsoft Forms surveys, and Silktide Accessibility scores, as well as to increase the share of digital over telephone transactions. Security and service reliability remain priorities, with a commitment to prevent high-security incidents and maintain high uptime for digital services.

11.2.2 The Applications and IT Procurement team's 2024-25 strategy includes implementing the Orbus Infinity platform to align IT with business needs, establishing new Oracle support contracts, and migrating all applications from Windows 2012 servers. Other notable projects are the Single View of the Child program, a central support model for critical applications, and the launch of Redwood forms for Oracle Cloud. Phase 2 of Microsoft 365, featuring Purview, secure email, and Teams telephony, is underway, alongside the migration of Business Objects reports to Power BI for enhanced analytics.

11.2.3 Achievements this year include the launch of new registration services, the migration of Lewisham's public website to Azure, and the deployment of a new Housing Management System. Applications and IT Procurement rolled out ORC for schools' HR, Egress Prevent for secure communications and launched a new intranet. Data Science achievements include the "Living in Lewisham" interactive map, enhancements to the DMT report, and a successful Local EV Infrastructure Fund (LEVI) application to support electric vehicle charging. ICT accomplishments include the migration of mobile services to O2 and live support for the Housing Management System.

11.2.4 Upcoming ICT Initiatives will focus on enhancing infrastructure reliability, improving service efficiency, and fostering innovation across departments, further supporting Lewisham's commitment to effective digital transformation and resident-focused services.

11.3 Southwark Digital Update

11.3.1 In October 2024, Southwark successfully launched the new council website, marking a significant milestone in its digital transformation journey. This was closely followed by the introduction of the new Cyber Security Training platform, aimed at enhancing the organisation's resilience against cyber threats.

Southwark's Modern Data Platform dashboards have been rolled out, providing advanced analytics and insights to drive data-driven decision-making across departments. Additionally, the Digital Skills Hub was launched, a dedicated platform to upskill the workforce and bridge the digital skills gap.

The technical evaluation for the new ERP (HR and Finance System) replacement has been completed, ensuring that the future system will meet

the evolving needs of the organisation. Furthermore, the WiFi infrastructure in office locations and libraries has been upgraded, enhancing connectivity and productivity for staff and visitors.

In terms of software procurement, Southwark has successfully reprocured Microsoft Licensing, which now includes 300 CoPilot licenses for the pilot of GenAI. This initiative is complemented by the Magic Notes Gen AI pilot in Social Care, which aims to leverage artificial intelligence to improve service delivery.

The new Project Management Office (PMO) has been implemented, supported by project management software (Monday.com), to streamline project oversight and execution. The Power Platform Centre of Excellence has also been established, fostering innovation and efficiency through the use of low-code solutions.

Lastly, Southwark has introduced UI Path RPA capability and capacity to the organisation, with four automations already developed and a robust pipeline for future opportunities. This initiative is set to significantly enhance operational efficiency and service delivery.

11.3.2 Expected Benefits

These initiatives are expected to bring numerous benefits to Southwark. The new council website and upgraded WiFi infrastructure will improve user experience and accessibility for both staff and visitors. The Cyber Security Training platform will bolster the organisation's defences against cyber threats, ensuring data security and compliance.

The Modern Data Platform dashboards will enable data-driven decision-making, leading to more informed and effective strategies. The Digital Skills Hub will empower employees with the necessary skills to thrive in a digital environment, fostering a culture of continuous learning and development.

The new ERP system will streamline HR and finance processes, increasing efficiency and reducing administrative burdens. The inclusion of 300 CoPilot licenses for the GenAI pilot and the Magic Notes Gen AI pilot in Social Care will harness the power of artificial intelligence to enhance service delivery and operational efficiency.

The implementation of the new PMO and the Power Platform Centre of Excellence will improve project management and innovation capabilities, ensuring that projects are delivered on time and within budget. Lastly, the introduction of UI Path RPA will automate repetitive tasks, freeing up staff to focus on more strategic activities and improving overall productivity.

11.3.3 Data

We're in year 3 of the data strategy. So far we have built a data platform that ingests multiple datasets visualising this data through a number of dashboards.

With this platform now in place and firmly established we are working with various departments to provide them with meaningful data in a way that offers them insight to improve and develop the services they deliver.

- The Modern Data Platform (MDP) holds information covering datasets from multiple back-office systems including:
  - 8x8 telephone contact centre system,
  - iCasework complaints system,
  - Universal Credit,
  - Mosaic Adults and Children's system,
  - Synergy Adults and Children's Case system,
  - Adult Learning,
  - Capita Youth Justice
  - 16 17 Not in Employment or Education or Training,
  - School Census
  - SAP financials,
  - ONS deprivation,
  - Gazetteer,
  - Meter Point,
  - Connect Repairs,
  - NEC Housing system
  - NEC Revs and Bens system

We are currently applying to work with the DofE and 12 other councils. The initiative aims to support up to 12 local authorities in developing an implementation plan for a single digital view of children and families. This involves effective multi-agency information sharing and joined-up working to safeguard children.

11.3.4 Single Digital View

This concept brings together information from various multi-agency case management systems into a unified view. It includes developing a data lake, implementing a match and merge management function, and visualising the information through

The resident account feature of "My Southwark" provides a limited single view of the customer by bringing together residents personal information and linking with Housing through an integration with NEC, Council Tax and the Blue Badge scheme. This helps the resident access disparate systems without the need for alternative logins

11.3.5 Digital Academy

The Southwark Digital Academy is currently offering several programs to help employees upskill and address digital challenges. One of the key programs is

the 'AI for Business Value' program, which covers AI fundamentals, AI ethics, business analysis skills, and how to embed AI into the organization. This program offers a government-recognised qualification (L4 Business Analysis). Additionally, there are fully funded Data/Business Transformation apprenticeships available.

We are training people in both formal qualifications as above and training to meet the organisation's needs. The Digital Academy runs training in how to collaborate effectively using Teams and OneDrive.

11.3.6 Social Value

Social Value remains a key priority for Southwark contracts and offers an opportunity for companies to work and contribute directly to residents and community organisations across Southwark. As part of their social value commitments, Infosys launched the Springboard platform at Canada Water Theatre this month. The launch was attended by Southwark residents, digital champions who volunteer and support residents with their digital skills, and members of the Libraries Teams.

The event was also an opportunity to express our thanks to the volunteer community who are the foundation of our digital inclusion skills sessions, offering their time, resources and patience to hundreds of residents every year. Springboard has over 1000 free courses available to residents to upskill and expand their digital and life skills and will be part of our digital inclusion offering going forward, supplementing the Digital Unite and Learn My Way platforms.

## 12 Inter Authority Agreement

12.1 Some revisions have been proposed to the IAA and these are to be presented to the Joint Management Board in January 2025.

12.2 We have been working with LOTI on benchmarking the IT service costs against other London Boroughs, to ensure that the shared service is providing value for money compared to the traditional model of an in-house IT team.

## 13 Strategy Update

13.1 Our existing SICTS Strategy was presented to the Joint Committee in January 2020.

## 14 Financial Considerations

14.1 The total budget of £18.12M for FY 2024/25 is made up of a combination of non-controllable expenditure of £9M and controllable expenditure (staffing and consultancy) of £9.12M.

14.2 The YTD spend (April 24 and October 24) for FY 2024/25 is £11.86M against a full-year budget of £18.12M. The forecast outturn for FY 2024/25 is ~ £18.1M, with a net underspend of ~ £30k.

14.3 The YTD Spend for the year excludes recharges which are made up of bulk stock orders, project costs that are covered by different funding pots and rechargeable consumables.

14.4 For FY25/26, we are committed to agreed savings targets through negotiations at contract renewals or replacement of contracts with those that provide better value. Our target for savings totals £900k.

14.5 We are currently waiting for the results from the value for money review, the London Office of Technology and Innovation are concluding a benchmarking exercise in which all three councils participated along side the shared service.

## 15 Legal Considerations

15.1 This report is for noting. Therefore, no specific legal implications arise from the report at this stage.

15.2 Brent Council hosts the Shared Technology 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.

15.3 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.

15.4 Joint Committees can in turn delegate functions to one or more officers of the councils concerned.

15.5 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.

## 16 Equity, Diversity & Inclusion (EDI) Considerations

16.1 Please not as referenced in 5.3 all STS staff are undergoing EDI training.

## 17 Climate Change and Environmental Considerations

17.1 There are none.

## 18 Consultation with Ward Members and Stakeholders

18.1 There are none.

## 19 Human Resources/Property Implications

19.1 There are none.

**Report sign off:**

***Minesh Patel***
Corporate Director Finance & Resources (Brent Council)

Dear Joint Committee member,

Please see below the briefing note on the global IT outage of Friday, 19 July 2024, caused by a CrowdStrike update.

Brent, Lewisham and Southwark are CrowdStrike customers. We have 934 Windows servers, of which 932 had the CrowdStrike agent installed. The servers received a routine update of the CrowdStrike client at approximately 5:30 on the morning of July 19, 2024. When the update was received, a logic error in the code, caused the servers to crash and the servers would not recover without manual intervention or restoration from backups.

At that point, when all servers crashed, essentially all councils' services were down for all, as authentication for anyone to log in was not available. Staff could log in to their laptops using cached credentials, but other services like Outlook, Teams, and front-line applications were offline. There may have been a few applications hosted by 3rd parties that may have worked, especially if they required a unique login and password, but fundamentally the council could not operate.

Brent and Lewisham's websites were up as they are externally hosted, but not all website services were available. Southwark's website was not operational until approximately 11:00 due to larger dependencies on other services that were offline. It was not until around 14:00 that most of the website features for all council websites were available when other application servers were restored.

The shared service discovered the issue around 6:30 am and put a team together, the team focused on Tier 0 services (Underpinning infrastructure, network connectivity, authentication etc), we spoke with CrowdStrike and received the information needed to recover the services, this took us until approximately 10:30 for Tier 0, from around 10:00 we started to recover Tier 1 applications (Social Care systems, Housing, ERP, Revs and Bens, etc) this took us until around 14:00, we were meeting with the councils every hour on the hour for the prioritisation of the recovery of services, we then focused on Tier 2 and 3 services (libraries, street cleaning, planning systems etc) which continued until around 18:30, almost all services had been restored but some additional servers were needed over this weekend and some more work although minor was still needed on Monday morning.

Our recovery methods were a mixture of what CrowdStrike provided, and in some cases where data integrity was not an issue, it was quicker to recover from a backup taken approximately 21 minutes before the crash, we were incredibly lucky with the timings of this incident as we had very recent backups also we had the CrowdStrike agent installed on laptops for council members and senior managers as additional assurance over the recent election period, the fact that most laptop users would have been offline when the software update was released meant that they didn't receive the update and we avoided a much larger issue.

In summary, council core services were unavailable from around 05:30 until around 10:00, when they started to recover until 14:00, and less critical services recovered between 14:00 and 18:30 and some bled over the weekend and Monday morning; if you have any specific questions about this incident, please feel free to reach out to me.

Fabio Negro
Shared Technology Services

This page is intentionally left blank

| | |
|---|---|
| | **Joint Committee of the London Boroughs of Brent, Lewisham and Southwark**<br>26 November 2024 |
| | **Report from the Managing Director of Shared Technology Services** |

# Briefing Laptop Refresh Project – Procurement process review

| | |
|---|---|
| **Wards Affected:** | N/A |
| **Key or Non-Key Decision:** | N/A |
| **Open or Part/Fully Exempt:**<br>(If exempt, please highlight relevant paragraph of Part 1, Schedule 12A of 1972 Local Government Act) | Open |
| **No. of Appendices:** | Three<br>Appendix 1: Further Competition Guidance<br>Appendix 2: Social Value Policy and Methodology included in the Tender<br>Appendix 3: Scoring Methodology |
| **Background Papers:** | None |
| **Contact Officer(s):**<br>(Name, Title, Contact Details) | Fabio Negro<br>Managing Director of Shared Technology Services<br>Email: Fabio.Negro@sharedtechnology.services |

## 1.0 Purpose of the Report

The purpose of this briefing is to demonstrate the processes and steps taken in the Laptop Refresh Procurement. These steps were to ensure most advantageous tender, value for money, social value and future proof solution for 5 years.

The table below outlines the high-level summary of the steps taken in conjunction with PCR2015, the guidance of the chosen framework and STS procurement protocols aligned to London Borough of Brent's Constitution.

| Tender Stage | Action | Responsible / Involved | Date |
|---|---|---|---|
| Pre-tender and governance considerations | Pre-Market Engagement: engaging with the market and shortlisting/benchmarking exercise carried out. Also followed the guidance in the preferred framework at that stage: RM6098 Market engagement best practice & process v2.7. | STS IT Department<br>Procurement & Commercial<br>Project Management<br>Partners (LBL, LBS, LBB & LGA) | Oct/Nov 23 |
| | OEM's shortlisted based on initial engagement with the market. STS drafted specifications. | STS IT Department<br>Procurement & Commercial<br>Project Management<br>Partners (LBL, LBS, LBB & LGA) | Nov 23 – Dec 23 |
| | Internal assessment of all OEM's. One OEM was shortlisted on the basis of which Supplier best meets the technical and pricing requirement.<br><br>Technical specification was in-depth to ensure capability with current infrastructure and market standards, and future proofing for 5 years to achieve best value for money and most advantageous tender. | STS IT Department | Feb / Mar 24 |
| | Shortlisting of different Frameworks concluded. | Procurement<br>Legal | Mar 24 |
| | Approval of route to market* using CCS Technology Products and Associated Services Framework RM6098.<br><br>***Gateway 1 report drafted and approved by Legal. Approving the use of the Framework, for further competition as recommended route to market. Suite of documents from Framework shared with Legal. Initial governance report encompassed all three Boroughs and LGA.***<br><br>The ***Further Competition**** - (Appendix 1) route to market was determined based on | Procurement<br>Legal | Jun 24 |

| | | | |
|---|---|---|---|
| | internal requirements and also following the guidance in the Buyers Guide of the chosen framework:  RM6098-Buyer-guide-v8.odt<br><br>Social value considerations were included within the tender as identified in **Appendix 2**. | | |
| Tender Stage | Tender (further Competition) was published through CCS Portal to shortlisted suppliers on Lot 1 of the above framework. | Procurement | Jun 24 |
| | Tender evaluation and moderation of scoring<br><br>8 evaluators involved of the technical methodology. Technical Questionnaire consisted of 41 questions, to ensure all details necessary were captured.<br><br>***Scoring Methodology – appendix 3****| STS IT Department<br>Procurement | July 24 |
| Contract Award & Governance | The Contract was awarded to the successful supplier following moderation.<br><br>Lead member of Cabinet approved Gateway 2 (authority to award)<br><br>Following authority to award approval, outcome letters were issued to both unsuccessful and successful supplier(s)<br><br>Voluntary standstill period was observed before signing of the contract.<br>No challenges were received during this period.<br><br>Contract awarded to successful supplier for duration of 5 years. Commencing 1st Sept 24. | STS IT Department<br>Project Team<br>Procurement<br>Finance<br>Lead Member<br>Legal | Aug – Sep 24 |

## Appendix 1 – Further Competition Guidance

### When to run further competition

A further competition is a thorough, open and fair method to find the best outcome for your requirements. CCS always recommends a further competition to be run over the other available buying options included within the framework agreement.

Your evaluation criteria can include weighted questions on price, quality and social value.

| **Criteria** | **%** |
|---|---|
| Price | Central Government 10-90%<br>Wider Public Sector 0-100% |
| Quality | 0-90% |
| Social Value | Central Government 10-90%<br>Wider Public Sector 0-90% |

When carrying out a further competition Central Government buyers must comply with the policy set out in PPN 06/20 by ensuring that they evaluate against social value requirements aligned with governments Social Value Model.

The social value question you include within your invitation to tender can be a pass / fail (yes / no) for simple and /or urgent requirements. We recommend forming your social value question around your organisation's values, objectives and ESG aims to gain the best value from this ensuring your are proportionate to the value of the contract.


Page 42

## Appendix 2 – Social Value Policy and Methodology included in the Tender

Appendix E1 - Social Value and Ethical Proc

Please explain your proposals for delivering Social Value to the participating organisations over the life of the contract. As the London Borough of Brent is the Contracting Body for this procurement, Brent's Social Value and Ethical Procurement Policy is appended separately (Appendix E1). This provides information on the council's themes along with examples of opportunities to provide Social Value. It should be noted however that the Supplier's Social Value offerings should be available to any or all participating organisations.

Explain how your disposal services deliver value through cost savings, social value, and service improvements. Include how you handle the resale of IT assets and reallocation of funds.

## Appendix 3 - Scoring Methodology

| The following marking scheme will be used to assess the response provided to this question: | |
|---|---|
| Score | Criteria |
| 0 | Weak submission that falls short of the requirements, is poorly explained and will not deliver the value required of the opportunity or no response received |
| 1 | Submission that meets only some of the requirements and will not deliver the value required of the opportunity |
| 2 | Satisfactory submission that meets the essential requirements and is explained adequately. |
| 3 | Good submission that meets all the requirements, is fully explained demonstrates the business benefits to be gained. |
| 4 | Very good submission that exceeds the required standard, is clear, fully explained and delivers additional benefit on many aspects of the requirement. |
| 5 | Very good submission that exceeds the required standard, is clear, fully explained and delivers additional benefit on all aspects of the requirement. |

# Shared Technology Services

# Strategy 2024-2026

# A word from our **Joint Committee**

## **Brent's** Lead Councillor
### *Mili Patel*

The shared service team has worked closely with Brent council's Digital and IT teams in delivering our strategy for Digital Transformation using a modern, flexible and scalable platform.

This STS 2023-2026 strategy continues to support Brent's plans to unlock efficiencies in operations across the council and contributes to our sustainability targets, whilst maximising our investment in the Technology Roadmap & further improving IT Service levels.



## **Southwark's** Lead Councillor
### *Stephanie Cryan*

Through partnership with STS, we aim to build a foundation to serve our residents better. STS' dedicated team of service tech experts is committed to delivering the best service solutions that will enhance the community's experience.

With STS, we can expect innovation, reliability, and a seamless partnership for a brighter, more efficient future.

## **Lewisham's** Lead Councillor
### *Amanda De Ryk*

Since partnering with STS in 2016, Lewisham's IT service has improved in stability and performance, but many challenges remain. Recent changes are benefiting us but recruiting and retaining talent is tough. STS is providing apprenticeships to nurture growing technology careers.

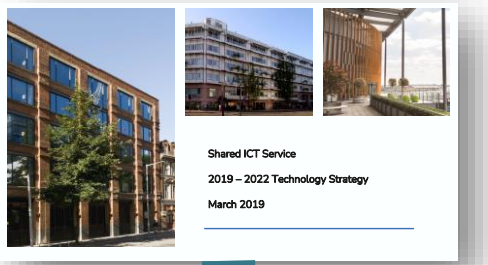
We will continue to work together to strive for an excellent, responsive, and adaptable delivery. Together, our partnership is stronger and more effective than individual efforts.

## **Shared Technology Services** Managing Director,
### *Fabio Negro*

Since joining the shared service at the beginning of 2020, I have watched the service mature and expand its capability.
Collectively with the councils, we have forged a lasting relationship that has allowed services within the councils to advance and react to challenging situations such as COVID.

Moving forward, I want the shared service to continue to focus on delivering more value to the councils, securely and robustly.
Decisions must be based on smart datasets that allow us to think outside the box, as we modernise the service, a shift from operations to innovation is critical.

# Our **Journey**




The previous strategy focused on building a **sustainable shared service** as it grew in a short period, improving stability and continuous improvement.

Since the previous strategy was written we have built **strong partnerships**, built a better platform to deliver services and confidence has increased.

Dealt with the impact of **COVID-19** pandemic

Delivered the foundation phase for **Azure cloud** programme

Delivered a **restructure**, added new capabilities such as Cyber and Service Design teams

Improved our **SLA** performance for Major incidents, and reduced the overall number of incidents and issues raised

Built the 5-year **STS Tech Roadmap** to 2025, and delivered Rubrik immutable backup and HCI Storage & Compute

Created the **STS Cyber Strategy** & managed cyber attacks and had **no serious incidents**

**Reduced** the cost per person by 13% in 3 years

**Onboarded** Lewisham Homes

Delivered the Southwark **datacentre migration** from Capita to Azure and on-premises




SharedTechnology.Services

# STS **Case Studies**

## Brent

We upgraded the Wi-Fi at Civic Centre to modernise connectivity for staff working at the office.

This uses Juniper MIST Wifi6 and is now being implemented in Southwark and Lewisham. The solution provides:

- Controller-free modern micro-services architecture.
- Elastic vertical and horizontal scalability.
- Deployment flexibility and cloud management.
- Marvis Virtual Network assistant performs root cause analysis for most detected network issues.
- Dynamically captures packets when an error occurs in real-time.
- Advanced alerting and Service Level Monitoring



## Lewisham

We replaced the legacy Compute and Storage solutions with best-of-breed Nutanix Hyperconvergence.

- **Scalable and agile** – Future proofed to meet the future needs of Lewisham and other partners.
- **Simplified management**. Management of the entire HCI stack is through a single pane view.
- **Security** - Improved network security and segregation through micro-segmentation.
- **Performance -** The disk storage consists entirely of SSD Flash disks so reducing read/write operation times.
- **Cloud compatible**
- **Reduced Power usage** & **Cost -** Smaller hardware footprint resulting in less power and cooling being required, so promoting a greener solution

## Southwark

To renew our backup capability, we implemented Rubrik Immutable backup solution:

- **Secure immutable backups** – this is a key requirement to allow the councils to be confident of their ability to be able to recover all data in a timely fashion in the event of ransomware attack. A recent breach has been reported as costing a local government authority over £10m to recover (Redcar-Cleveland Data Breach)
- **DR provision in the cloud** – this gives us more options in when reviewing DR datacentre requirements
- **Small datacentre footprint** - A “greener” solution to help meet sustainability targets.
- **Reduced administration** – Simpler to manage, reducing overhead on operational teams.

# How we **Work Together**

## What **STS** manages for all Partners

STS provide the foundation of IT in the partner councils and manages the processes shared by all.
These are the **core elements** required to run the IT function of any organisation.

| STS Managed Functions | | |
|---|---|---|
| IT Service Desk | Internet Connectivity | Procurement |
| Directory & Identity | Office Connectivity | Service Improvement |
| Datacentre Hosting | Remote Access | Problem Management |
| Cloud Hosting | Email | Change Management |
| Firewalls | IT Security & Monitoring | Capacity Management |
| Data Storage | Collaboration tools | Availability Management |
| Data Backup | End User Computers | Disaster Recovery Planning |
| Fixed Telephony | Remote Access | |
| Mobile Telephony | | |

## What **Partner Councils** manage

The partner councils retain ownership of information, applications and digital services.
These are tailored to best meet **staff & residents' need**.

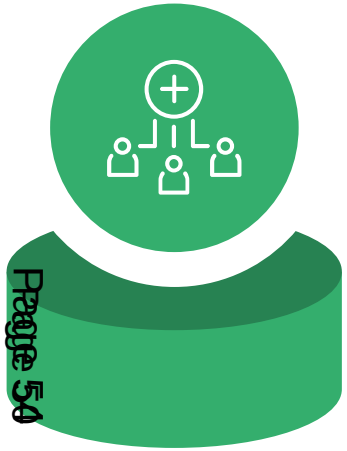
| Partner Council Managed Functions |
|---|
| Information Governance |
| Application Security & Support |
| Application Strategy |
| Digital & Web Development |
| IT & Security Policies |
| Meeting Room Audio/Visual |



Brent Lewisham Southwark

# Our **Values**

"As Shared Technology Services our core values drive and guide us as we serve the organisations we support."



## COLLABORATE

We are dedicated to a constructive, team-oriented environment, gathering varied perspectives, sharing knowledge and building effective partnerships with key stakeholders.

## IMPROVE

We strive for operational excellence through the on-going development of our team.

We encourage creative thinking and constructive challenge in the development of technology services, solutions and operational processes.

## CARE

We listen to, respect, care for and equally treat our staff, customers and one another, both professionally and personally.

## SERVE

We strive to provide excellent service by being fair, consistent, agile, reliable and accessible to all.

Make every contact count.

## BE OPEN

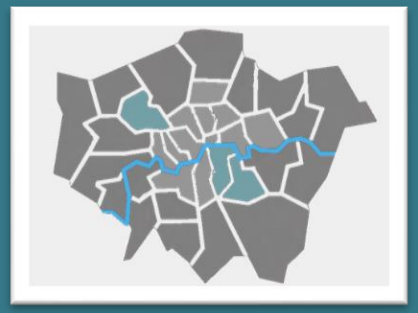
We leverage open communications and thoughtful business processes to be accountable in our interactions and our work.

# Our **Vision** & **Mission**

## Our **Vision**

We will deliver an **outstanding**, public sector technology service for the benefit of our organisations.

We will build our brand and reputation to be recognised as being the **leaders** in London.



## Our **Mission**

To provide a **secure**, **reliable** and **cost-conscious** service which always strives for **improvement**, enabling our partners' digital ambitions.

# Our **Challenges**

The pressures in local government are common across the country.

The challenges highlighted are the foreseen obstacles we must manage to deliver this strategy.

Some of these challenges are expected to become more severe as we progress through the delivery of the strategy, others we will be able to control with mitigations in place.

- Financial pressures & Local Government spending cuts
- Post-COVID working expectations for remote/hybrid working
- Climate emergency called: services need to be sustainable
- Keeping up with the pace of technology change (e.g. Artificial Intelligence, Cyber security threats)
- Providing the foundation for increased reliance on data, integrations &  customer experience

# Our **Partnership**

The service has succeeded where others haven't, but we should always be mindful of how other shared services have failed in the past:

- Different ambitions & strategies
- A breakdown in relationships
- Mistrust between partners
- Financial pressures

- We must continue to build strong relationships and ways of working, with ever-changing stakeholders in all organisations: new executive directors, new CEOs, etc.
- STS and Partner IT teams need to continue to work collaboratively, and not fall into "Supplier / Customer" behaviour.
- Partners should  seek to work together on common needs outside of the shared service arrangement.
- STS needs to continuously demonstrate its value, with regular market comparisons.

# Our **Approach**

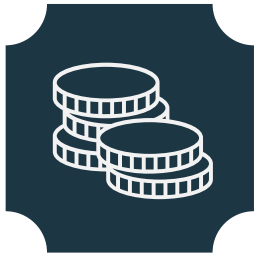
The focal points of this strategy will be:

- Providing an improved, responsive service to our partners
- Delivering our Technology Roadmap
- Protecting our data and the service we deliver from cyber incidents
- Making sure that every pound that is spent is on value
- Ultimately having a stable team that is enabled to use the tools they need to deliver the best outcomes for our residents.
- Ensuring we do our bit to protect our environment and ultimately our planet

In the following slides, we look at these areas of focus further.

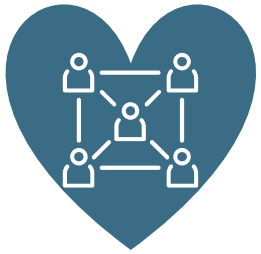


Cyber Security



Financial Value

Service & Technology



Wellbeing

Environment

# Service & Technology

## Our **Challenge**

- Technology evolves over time, and our original roadmap needs to evolve with it.
- Social Value isn't included in many of our existing contracts or procurement frameworks
- Our service levels, particularly for Priority 3 & 4, have not met our targets.
- Responsibilities between STS and partner teams are still ambiguous in some areas.

## Our **Objectives**

- Refresh our roadmap annually to reflect significant changes to the landscape, e.g. E5 licenses. Deliver the STS Technology Roadmap objectives.
- Maximise the opportunity for Social Value elements in our major contracts.
- Meet our SLA for P3 & P4 by understanding the underlying causes.
- Improve clarity for strategy, policy and operational responsibilities so that processes are defined and efficient.

## Our **Commitments**

- To implement major elements of the Technology Roadmap, actively monitoring costs against budget during delivery of projects.
- To include a social value element to contracts exceeding £1Million.
- To unlock our ability to analyse service management data and improvements to reduce P3 & P4 demand & meet our service levels.
- To identify and agree on key RACI models with all ICT teams for strategy, policy and operations.
- To develop a new Strategy Technology Roadmap for 2026 and beyond.

# Cyber Security

## Our **Challenge**

- As public sector we are always under cyber-attack for financial gain, political positioning or retaliation to an event with the council.

  These attacks are increasingly sophisticated, and we need to ensure that we are ahead of the attackers.

  Implications of this could be incidents valued in the multi-millions of pounds, ICO penalties and loss of data which could affect the wellbeing of our residents.

## Our **Objectives**

- Refresh the Cyber Security Strategy in 2023.
- Continuously develop the Cyber Security team in skills & resources and assess our Cyber maturity with an ongoing action plan.
- Actively participate and contribute to forums and seek out information to stay ahead.
- Invest in the right tools needed to protect our organisations with the 2021-25 Tech Roadmap.
- Ensure that we have the policies, processes and reports in place.
- Ensure that Disaster Recovery exercises are carried out.

## Our **Commitments**

- To minimise the risk of data breaches & the risk of disruption.
- To identify & deliver remediation actions promptly.
- To promote the importance of cyber security to our STS team and user community, instilling cyber security culture change.
- To be fully complaint in all regulation.
- To assure confidence in the service from our Audits.
- To mature the service so that it can provide advice and guidance to other external bodies.
- To be publicly recognised for our competence and knowledge.

# Financial Value

## Our **Challenge**

- Financial pressures, Local Government spending cuts, exchange rates, post-Brexit issues of importing goods.
- Global inflation & semiconductor prices increasing, although the chip shortage has eased during 2022.

- Increasing costs and decreasing budgets in the above means we have to be innovative in our operating costs.

## Our **Objectives**

- Monitor the impacts of global economic changes report and model to ensure we gain value for money.
- To contribute to Partner MTFS and deliver savings & value.

- Work with assurance partners to ensure where best-of-breed products are necessary and where more cost-effective solutions allow us to achieve our objectives
- Manage the pressure of high turnover within the organisations and within STS.
- Ensure that subscription & asset management are maintained and improved to ensure maximum efficiency.

## Our **Commitments**

- To ensure that we plan for economic changes and avoid unnecessary expenditure, taking advantage of collaborative commercial exercises with other councils to maximise economies of scale .

- Work with partners to maximise procurement on a best-value basis through standardised solutions.
- To operate with an appropriate buffer for both subscriptions and devices.

# Wellbeing

| Our **Challenge** | Our **Objectives** | Our **Commitments** |
| --- | --- | --- |
| Maintaining our skilled workforce with the rise in the cost of living and low unemployment, reducing our salary competitiveness. | That every team member feels valued, shares in our successes, and are not unduly overworked by maintaining a healthy work-life balance.<br>Promote from within when possible, with a clear succession plan for key roles. | To hold 1-2-1 meetings & invest in skills training, with managers ensuring the development of personal development plans.<br>To engender a culture of healthy wellbeing & manageable workload across all teams, with adjustments to headcount as needed. |
| The employee survey shows mixed results within the STS teams. | Employee survey results show consistently high job satisfaction, being noted as a 'good place to work'.<br>To provide opportunities for local people, via apprenticeships. | To undertake annual temperature checks on team wellbeing and job satisfaction.<br>To have evidence of career progression within our team.<br>To recognise and reward outstanding team member performance. |
| Post-COVID, does the team have access to the right tools and can we be attractive for external recruitment? | Ensure that the team have access to the training & tools.<br>Salaries are competitive for our sector and geography. | To regularly re-evaluate roles & salaries based on our market. |

# Environment

## Our **Challenge**

- As an IT service, we utilise a lot of energy to provide services; these are not always the most environmentally efficient way of delivering a service and produce more carbon into the air than we would hope for.
- We are responsible for a lot of devices which are provided to the workforce from cables & laptops to core infrastructure in the buildings that we support; these all come with packaging and materials which in some cases are not recyclable.
- Due to our scale, we have many devices that become end-of-life or are unrepairable.

## Our **Objectives**

- Identify and review areas where improvements can be made around a reduction in carbon, taking a step-by-step approach.
- Identify and review areas where improvements can be made around a reduction in energy consumption.
- Work with existing manufacturers to reduce none recyclable materials, ensuring what materials we can recycle are and following the appropriate guidelines
- Work with organisations to ensure that equipment can be redistributed to other needs instead of contributing to landfill.
- Work with suppliers to contribute via Social Value to supporting local environmental issues.

## Our **Commitments**

- To reduce the energy consumption in our datacentres by 40%
- To reduce carbon emissions for the normal operation of the service by 35%, also considering power efficiency when selecting new hardware & reducing the need to travel.
- To work with suppliers where possible so that all packaging is delivered to us with recyclable materials and ensure that they are recycled.
- To redistribute all our end-of-use devices to the digitally excluded, enabling further use.
- To recycle end-of-life devices & contribute to the closed-loop supply chain.

# Our **Future** Journey

Develop the future Technology **Investment Plan**

Implement the 2021-25 **Technology Roadmap**

Have evidence of **career progression** within our teams.

Maximise **procurement** on a best-value basis

Embed a culture of **healthy wellbeing** & workload

Reduce PUE per user

Include **social value** in major contracts

Be **publicly recognised** for our cyber security competence and knowledge

Redistribute our end-of-use devices to the digitally excluded

Undertake annual **temperature checks** on team wellbeing and job satisfaction

Work within **buffer** for subscriptions & devices

Identify & deliver **remediation** actions promptly

**Recognise & reward** outstanding team member performance.

**Refresh** the Cyber Security Strategy

Understand what drives demand & reduce **P3 & P4 instances**, whilst improving service levels to SLA.



- This strategy is focused on developing a **secure, reliable and cost-conscious service** which always strives for improvement, enabling our partners' digital ambition
- We will build our brand and reputation to be recognised as the **leaders in London**

SharedTechnology.Services

SharedTechnology.Services

November 2024

This page is intentionally left blank

# Shared Technology Services Cyber Security Strategy 2024-2026



# Ciarán Weldon
## Chief Information Security Officer
## Shared Technology Services

I am the Chief Information Security Officer (CISO) for the shared service and have over 20 years of industry experience.

I have worked in public sector IT for over 20 years; while at Brent and subsequently in STS, I was responsible for developing the Messaging and Cloud Services for the councils. These roles provided me with insights into security from several areas and provided me with the skills to build upon my role as CISO.

As CISO for the past two years, I have sought to build and expand the service's capabilities to address the ever-evolving daily threats. I am motivated to achieve a culture of collaboration within the service and with our partners. Ensuring we provide the best security to our staff and residents.

This renewed Cyber Strategy reflects the development of our Cyber Security service under my leadership. It paves the path for continued growth in deploying controls and policies, aligning the service with the NCSC strategic tenants of Defend, Deter and Develop. The foundation of the strategy is that Cyber Security is everyone's responsibility, and we are working in partnership with the councils to adopt this awareness.

Since the conception of the shared service, I have noticed a significant change in the threat landscape, with attacks becoming more targeted and sophisticated. Adaption of navigating the compliance requirements and regulatory standards specific to the UK government and, more importantly, keeping data secure and protecting residents needs to be continuous. This Cyber Strategy reflects the change in STS cyber posture and gives us the vision to protect councils and data by being more agile and reactive to adversaries.

Cyber Security is everyone's responsibility.

# 1. Introduction

Shared Technology Services (STS) is an IT shared service for the Brent, Lewisham, and Southwark councils.

Brent Council is the host borough for the service. STS is governed by an Inter Authority Agreement between the three councils and a Joint Committee of two 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.

Our cyber security commitment is to the residents of the three partner councils. It emphasises the importance of cyber security in the role of all staff.

# 2. The Challenge

Cybersecurity is a critical concern for local governments to protect sensitive information, critical infrastructure and essential services.
We have seen with increasing frequency how organisations can be impacted by cyber-attacks and the reputational damage that can follow.

For STS, the risk is threefold, as each council is subject to threat. Our original STS Cyber Security Strategy 2021-2024 outlined our approach of a continual cycle for protecting the councils and their customers from cyber-attacks, which remains our strategy for the next three years:

By implementing this revised, comprehensive cybersecurity strategy, STS can enhance cyber resilience, protect sensitive information and ensure the continued delivery of essential services to the community. Regular reviews and updates to the strategy ensure its effectiveness against evolving cyber threats.

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

Cyber incidents are on the rise, especially within the public sector. The ramifications are serious and widespread, from personal to economic. Protection and remediation are service disruption and 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 STS shall be adopting for our councils and customers. It is imperative that the right controls are put in place to protect and react to cyber threats going forward. STS have a strong relationship with the National Cyber Security Centre and other private cyber agencies which will harness to help protect the data of both citizens and customers.

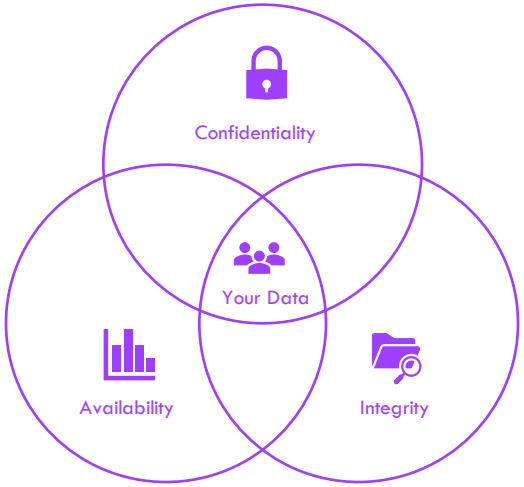
# 3. Why is cyber security important?

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 as 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 ~~to~~ effectively deliver services. Data is processed and stored in large amounts 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.




Sensitive data is transmitted across networks and to other devices, whilst providing services or even just using the 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 services are kept up and running. It is also vital in ensuring building and keeping the public's trust. A cyber-attack would have very serious consequences in terms of a disruption to services (many of which serve some of the most vulnerable residents), council's reputation and the impact to fiscal position.

# 4. 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 update introduces a 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, STS will comply with and embed the principles of the Cyber Assessment Framework; 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, with the data on the systems an STS responsibility, along with the services they help provide. The recommendations in this strategy will be embedded in all areas of new and emerging technologies which STS implement. It will also set out the best practices that will be rooted in business as usual.

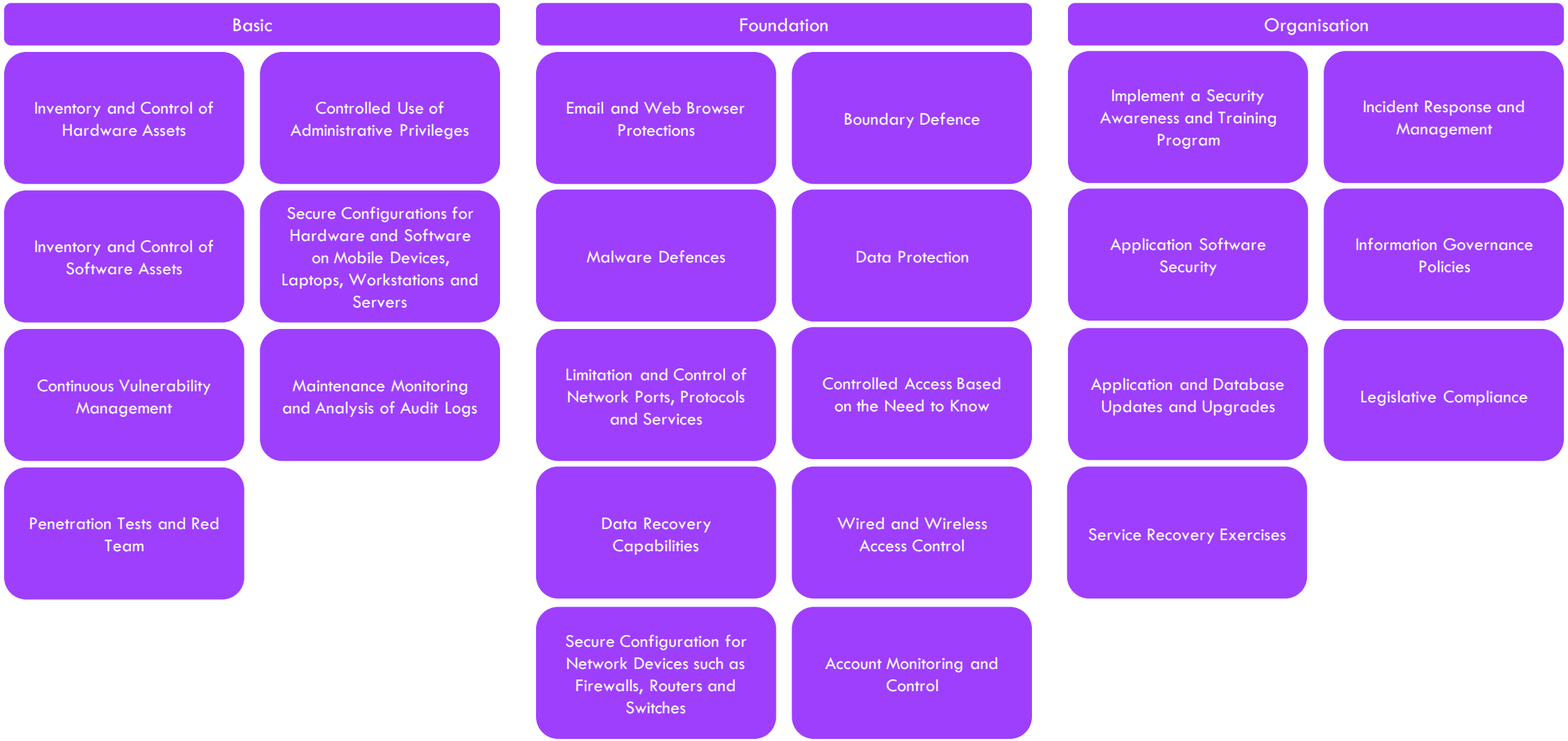


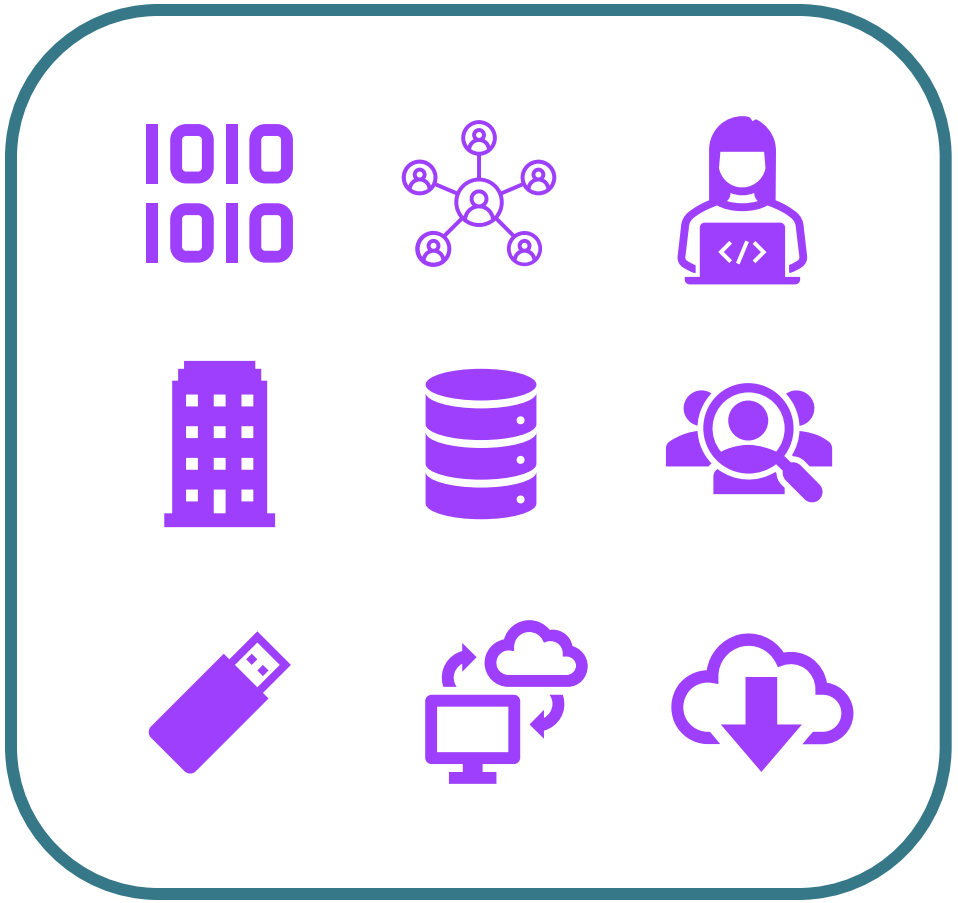

Figure 2 - The building blocks of Cyber Security

# 5. 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

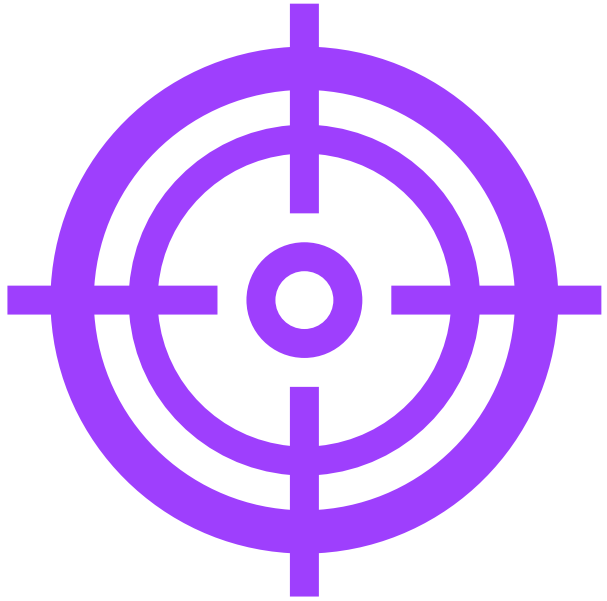


# 6. Vulnerabilities

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 affect data security adversely.

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

- **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 how an organisation installs and maintains its IT hardware and software components are threats.
- **Legacy Software** – To ensure that legacy systems have sufficient user and system authentication, data authenticity verification, or data integrity checking features that prevent uncontrolled system access.
- **Trend Analysis** - Monitoring organisational working patterns to identify unusual behaviour and respond accordingly.
- **Training and Skills** – It is paramount that all employees have a fundamental awareness of cyber security to support this.



# 7. Threats

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

Generally, there are two types of threats Insider Threats and Outsider Threats.

These threats are explained in detail in the chart to the right.



| | Insider threats | | Outsider threats | |
|---|---|---|---|---|
| WHO | Employees | Contractors | Cybercriminals | National state-sponsored attackers |
| | Business Partners and 3rd Parties | Compromised internal accounts | Competition-sponsored attackers | Hacktivists |
| MOTIVE | Financial gain | Personal advantage | Economic gain | Corporate or nation state-sponsored espionage |
| | Professional revenge | Outsider influence | Political advantage | Political or social change |
| TARGET | Intellectual property | Business plans and corporate information | Intellectual property | Business plans and corporate information |
| | Personal Information | Financial Information | Personal Information | Financial Information |
| METHODS | Social Engineering | Physical theft | Social engineering | Hacking |
| | Privilege abuse | Copying or offloading sensitive data to personal accounts/ drives | Malware | Denial of Service Attacks |
| | Unintentional data leaks or loss of company property | | Malicious USB drops | Physical theft |

## Cyber Criminals

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 cyber-attacks regularly disrupt online services, this could erode public confidence in such services.

Hacktivist groups have successfully used distributed denial of service attacks to disrupt the websites of several councils to date. (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 to sell to another party, but oftenly 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 software weaknesses are discovered. At that point, it's exploited before its creator makes a fix available. 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.

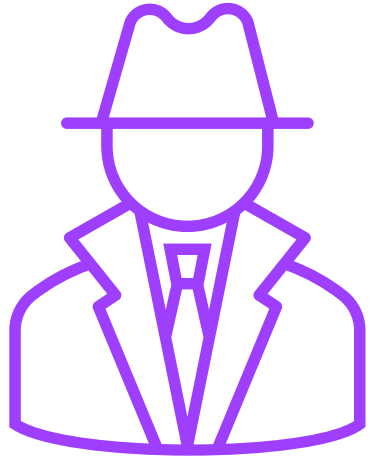
## Physical Threats

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

## Terrorist

Some terrorist groups demonstrate intent to conduct cyber-attacks, but fortunately have limited technical capability.

Terrorist groups could obtain improved capability in several ways, namely through the sharing of expertise in online forums providing a significant opportunity for terrorists to escalate their capability.



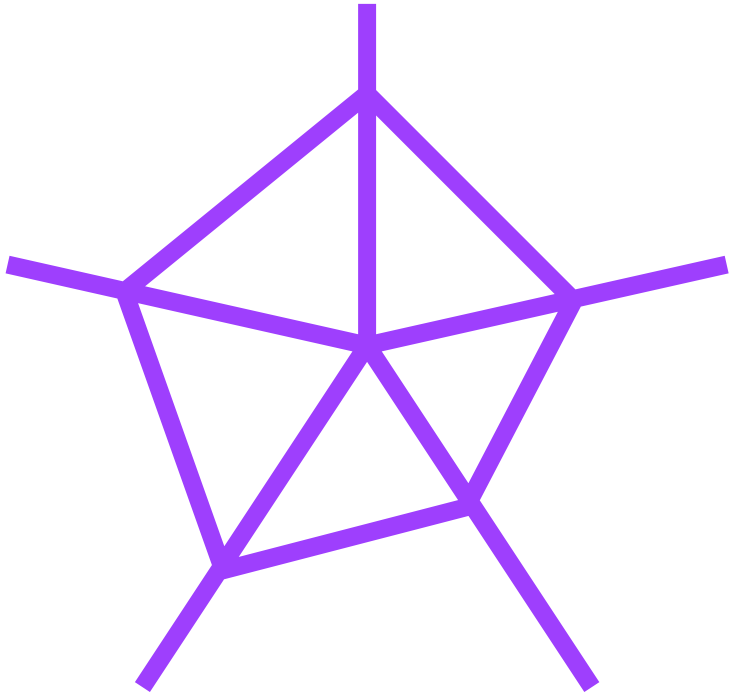
## Espionage

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.

# 8. 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. We conduct regular thorough risk assessments to identify potential vulnerabilities and threats specific to the local government's systems, networks and data. Regularly updating our assessments to stay current with evolving threats.



# 8. Our Approach

To mitigate the multiple threats, It is vital to face and safeguard  interests, a strategic approach that underpins the collective and individual actions in the digital domain over the next three years is required. This will include:

- Collaborate with the other technical and governance teams in the councils to ensure there is a cohesive approach to cyber security.
- Foster a culture of empowerment, accountability, and continuous improvement.
- Prioritising information assets and processes with 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.

To further enhance the maturity and capability of the service STS have enhanced the Cyber Security team within the Shared Service to take on responsibility for patch management and remediation plans.  STS's ability to rapidly and efficiently manage this will help to further reduce the risk to data; many of the more publicised incidents have been as a direct result of utilising where known weaknesses have not been patched in a timely manner.

The STS strategy also includes the initiation of a 24x7x365 Security Operations Centre service, via a 3rd party, to continuously detect and respond to attacks in real time; whilst having a limited service already for the server estate, the threat of attack is a global phenomenon, and therefore being always prepared and ready is a must.

# 9. Plan

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

It was recognised that each partner and council will be at different levels of maturity and capacity therefore STS developed a 3-year (2024-2026) Technology Roadmap which has already resulted in investment in a significant number of cyber protections.

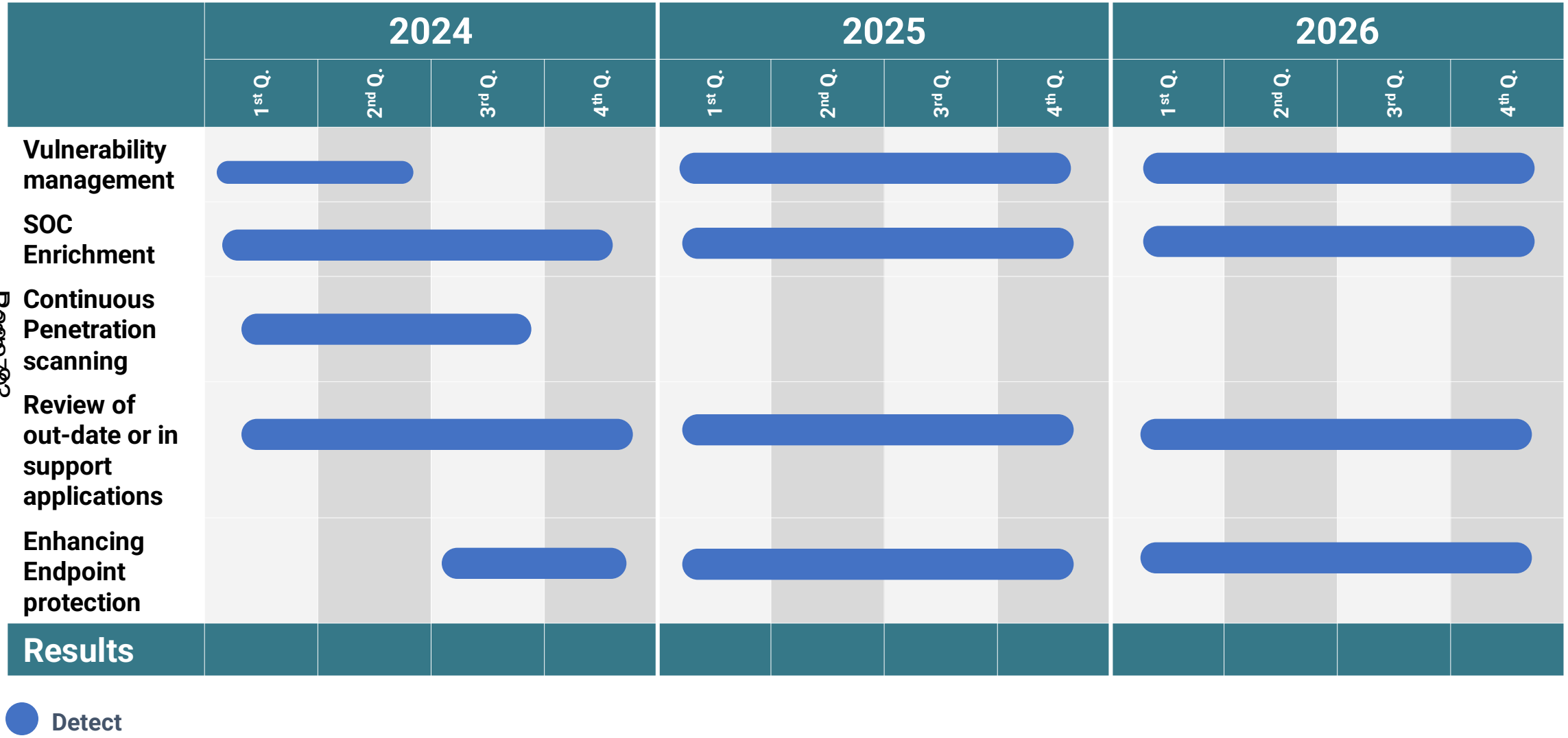
The 'Cyber RAG status' to assess our maturity in all areas has since been developed.

The STS implementation plan will recognise areas of improvement and put in place activities to address these, some of which will be a sovereign partner task, such as policy development. This will be an ongoing improvement plan.

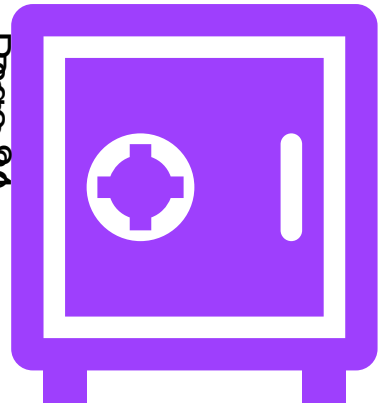
# 10. Detect

The preemptive detection of potential cyber events is the foundation of the strategy. Through the following stages:

**Asset Management:** Identify all the assets within the network, including hardware, software, and data repositories.
**Baseline Establishment:** Establish a baseline for the regular activity on the network, systems and users by introducing agents to monitor the network to greater effect.
**Threat Intelligence:** Using threat intelligence feeds and courses to understand the threats to our network and prepare defenses.
**Anomaly Detection:** Deploying agents to understand and detect deviations from normal behavior and the capability to respond to these detections.
**Continuous Monitoring:** Automated monitoring tooling continuously monitors network alerts and suspicious behaviours.
**Incident Response:** Develop and implement incident response plans and carry out tabletop exercises to outline the process and procedures to contain, mitigate damage and return services to normal operations.


2024
2025
2026
1st Q.
2nd Q.
3rd Q.
4th Q.
Vulnerability management
SOC Enrichment
Continuous Penetration scanning
Review of out-date or in support applications
Enhancing Endpoint protection
Results
Detect

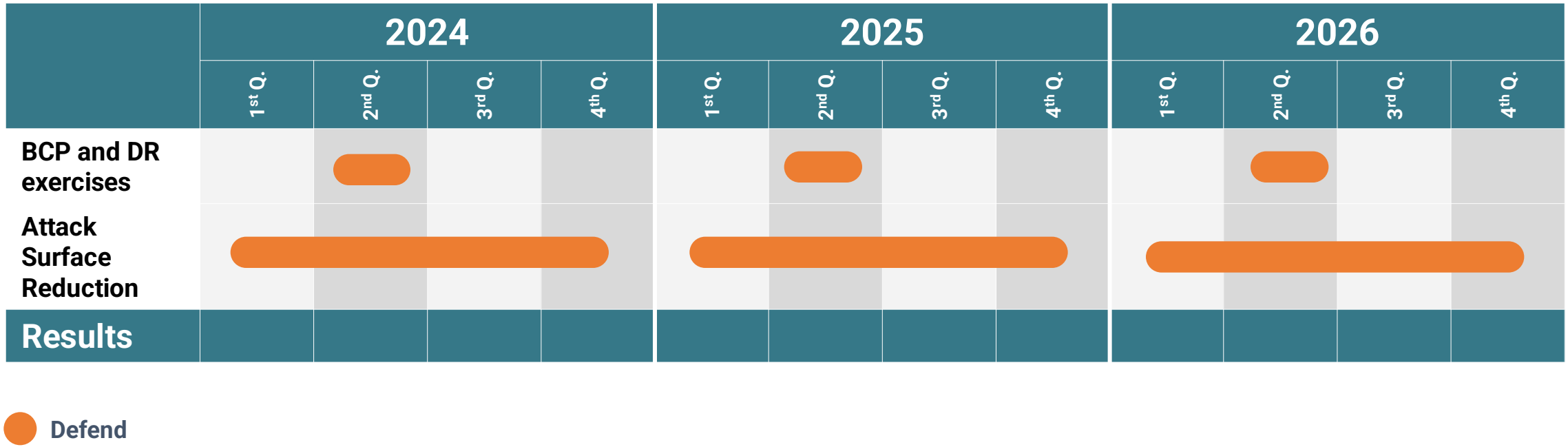
# 11. Defend



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 monitor 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, to provide assurance on 3rd party supply chain risk.
- Work with councils and customers to ensure websites and line of business systems are kept secure.
- Enhance our 3rd party Security Operations Centre service with a 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.
- Identify an STS Red team to be able to respond to incidents and have relationships in place with government agencies and cyber specialists.
- Assuring our DR plan by carrying out 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 (WARPs) and participating in Cyber resilience exercises with LOTI.
- Work towards ISO27001

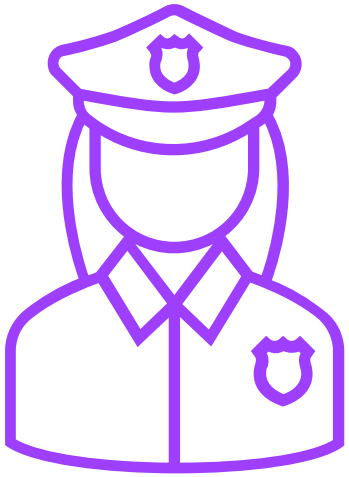

2024
2025
2026
1st Q.
2nd Q.
3rd Q.
4th Q.
BCP and DR exercises
Attack Surface Reduction
Results
Defend

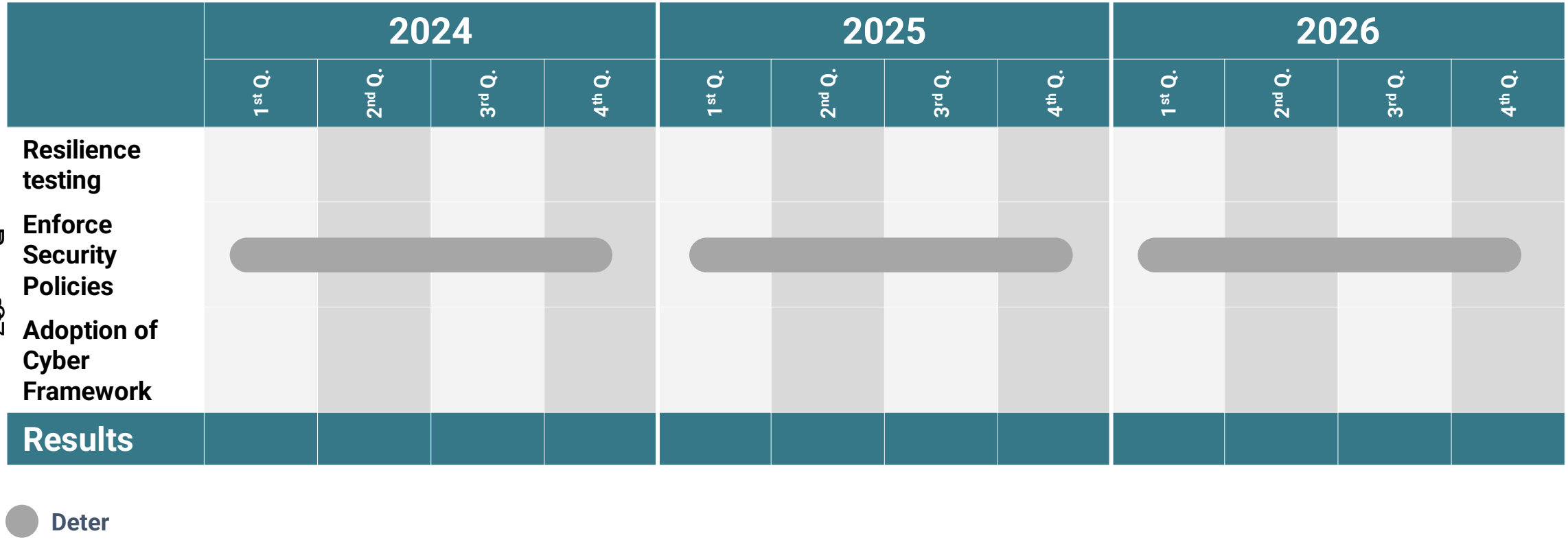
# 12. Deter

STS partner 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 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 latest 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.
- Enhancing our Security Operations Centre (SOC).




2024
2025
2026
1st Q.
2nd Q.
3rd Q.
4th Q.
Resilience testing
Enforce Security Policies
Adoption of Cyber Framework
Results
Deter

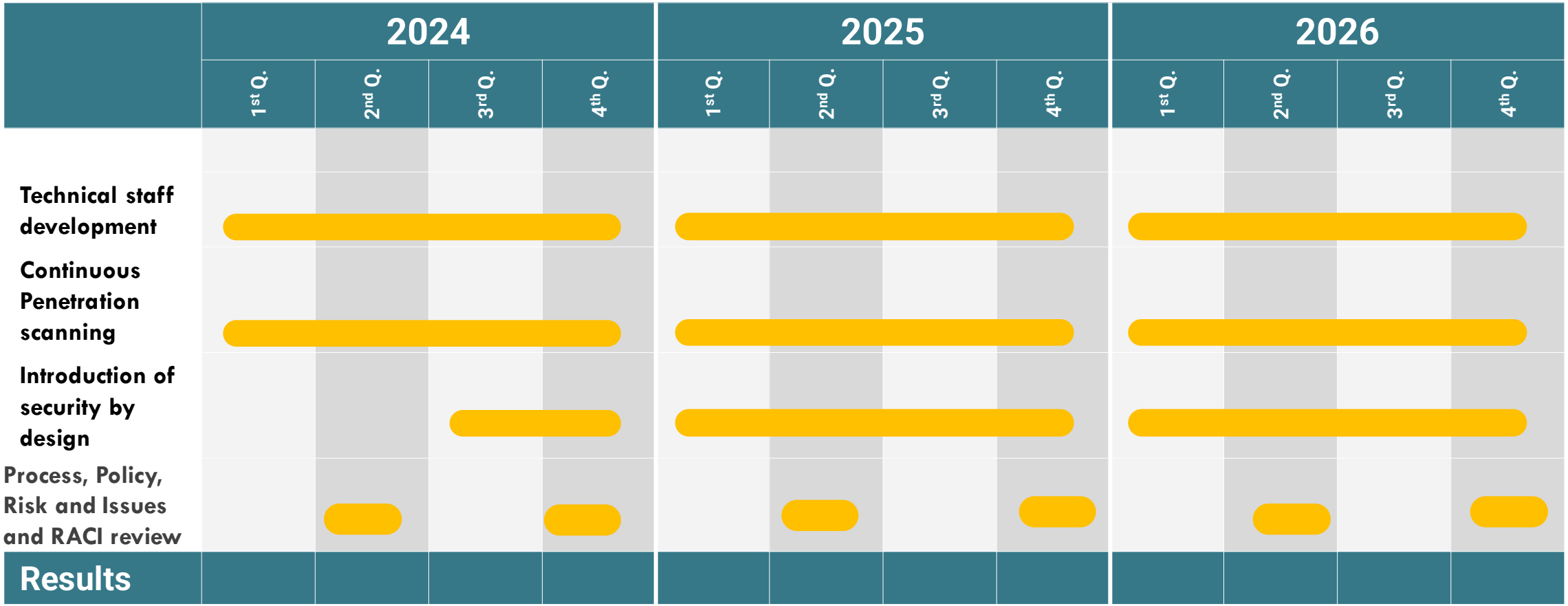
# 13. Develop



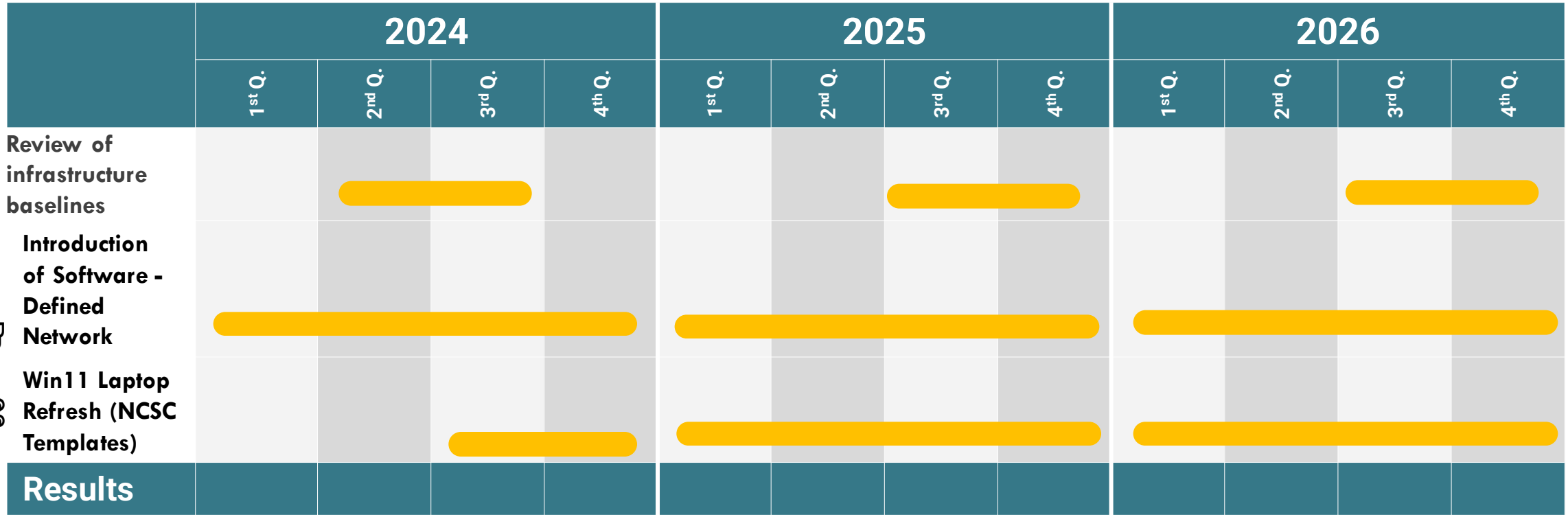
This includes developing a coordinated and tailored approach to risks and threats that we may encounter and mitigate potential vulnerabilities.

Actions:

- Develop and maintain risk management framework, internal control and governance for the prevention and detection of irregularities and fraud.
- Develop and enforce comprehensive cybersecurity policies and procedures that cover areas such as data handling, access control, incident response, remote work, and third-party vendor management. Ensure that employees and stakeholders are educated about these policies.
- 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
- Regularly train all staff and Councillors on cybersecurity best practices, social engineering awareness, and safe online behaviour. Conduct simulated phishing exercises to gauge the effectiveness of training and to identify areas for improvement.
- Regularly test and review our incident response and management plan, with clearly defined actions, roles, and responsibilities.
- Update our incident response and management plan to develop a detailed incident response plan that outlines the steps to be taken in the event of a cyber incident. This plan will cover identification, containment, eradication, recovery, and lessons learned. Regularly test and update the plan through simulated exercises.
- 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)
- Assess the cybersecurity posture of third-party vendors and contractors that have access to the local government's systems and data. Ensure that they meet our cybersecurity standards and follow secure practices.
- 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.


2024
2025
2026
1st Q.
2nd Q.
3rd Q.
4th Q.
Technical staff development
Continuous Penetration scanning
Introduction of security by design
Process, Policy, Risk and Issues and RACI review
Results

Develop


2024
2025
2026
1st Q.
2nd Q.
3rd Q.
4th Q.
Review of infrastructure baselines
Introduction of Software - Defined Network
Win11 Laptop Refresh (NCSC Templates)
Results

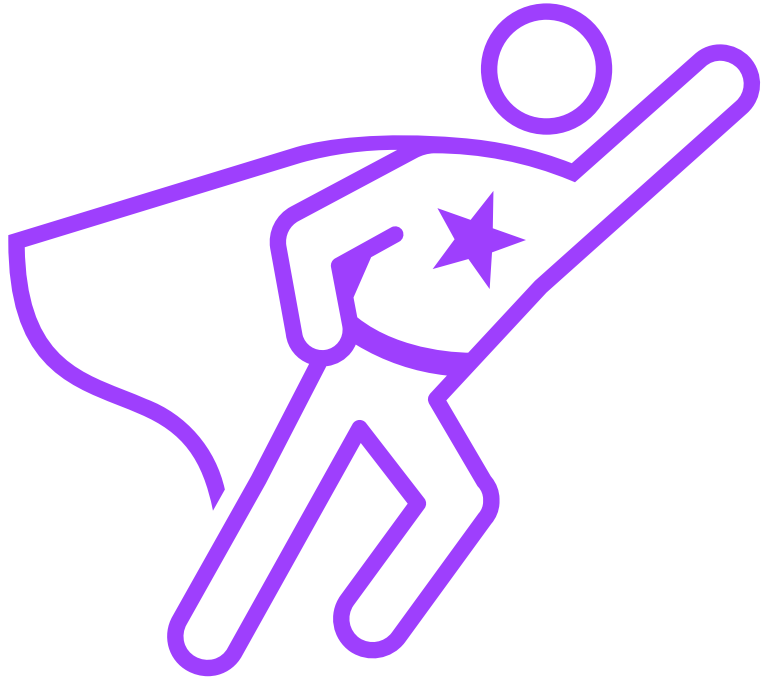


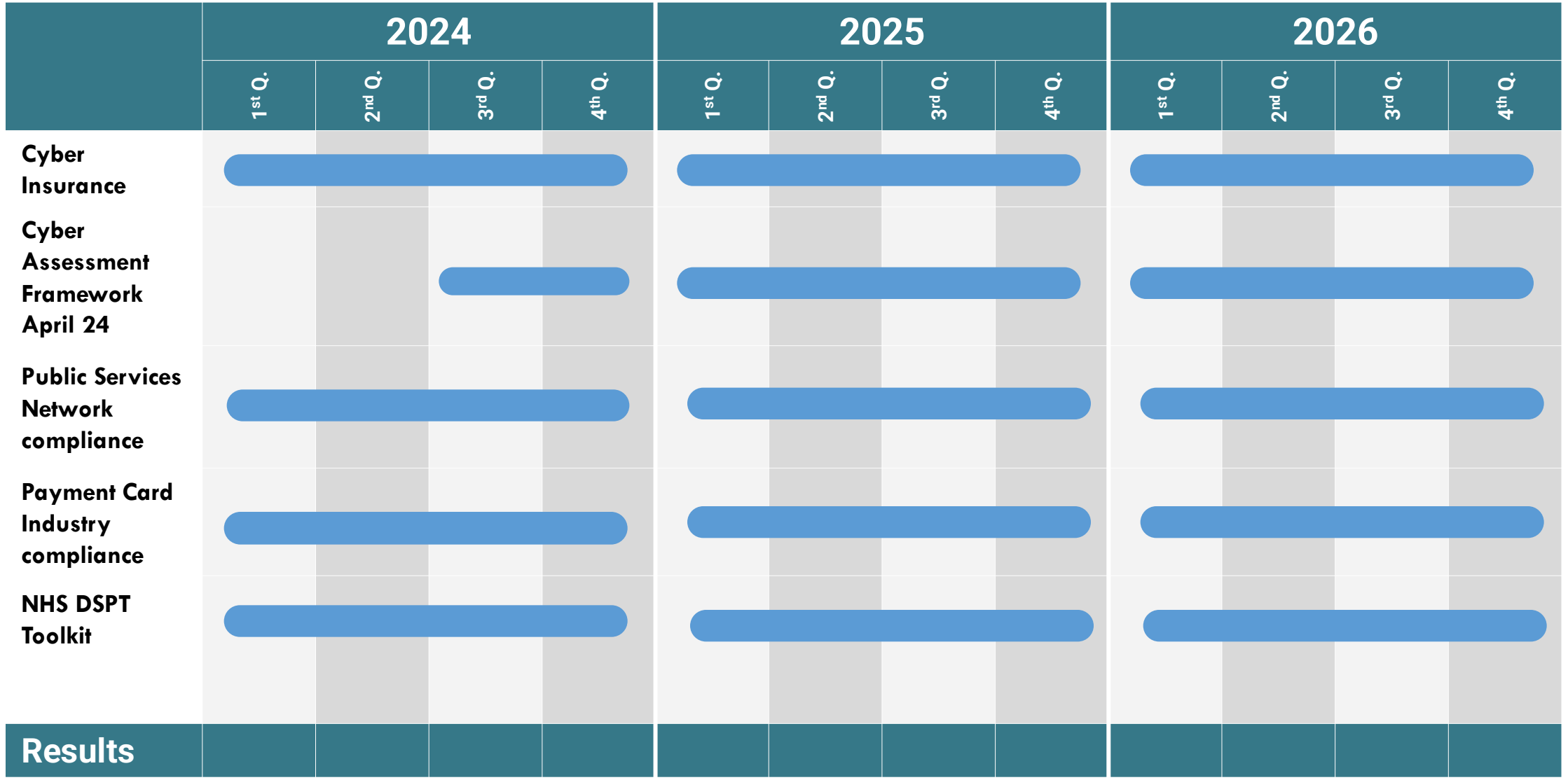
Develop

# 14. React

STS will ensure that sufficient controls are 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.

STS have third parties proactively monitoring our environment disabling any potential threats and locking down resources which are identified as a risk, which we will further enhance with a Security Operations Centre (SOC) service.




2024
2025
2026
1st Q.
2nd Q.
3rd Q.
4th Q.
Cyber Insurance
Cyber Assessment Framework April 24
Public Services Network compliance
Payment Card Industry compliance
NHS DSPT Toolkit
Results
React

# 15. 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.

# 16. Roles and Responsibilities

Information Governance and Policy will remain the councils' responsibility, 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 Group (OMG)

The Operational Management Group 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.

### STS Security Forum

The STS Security Forum is comprised of Information Security leads from each of the councils and the STS CISO, where they will discuss all technical controls, policy and process.

### 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.

### All council officers and Members

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

Document is Restricted