Meeting Name:	Audit, Governance and Standards Committee
Date:	1 November 2024
Report title:	Cyber Security Update
Ward(s) or groups affected:	N/A
Classification:	Open
Reason for lateness (if applicable):	N/A
From:	Dionne Lowndes, Chief Digital and Technology Officer Fabio Negro, Managing Director, Shared Technology Services

RECOMMENDATIONS

1. That the committee note the actions being taken in response to the BDO Audit, and their current status.

2. That the committee note that Shared Technology Service have procured a managed Security Operations Centre (SOC), with transitioning beginning in November 2024, to provide more comprehensive security coverage and capability, further strengthening our resilience.

BACKGROUND INFORMATION

3. This report provides an update on the work done to address the findings identified in the BDO Cyber Security Audit, dated August 2024.

4. We have committed through our Digital & Technology Strategy 2024-2026, Southwark 2030 and the Council Plan to continually improve how we manage our technology and digital services as being crucial to responding to local needs, operating with reduced budgets, and adaptive to changes in the technology world.

5. By prioritising cyber security, we can prevent potential threats, minimise risks, and ensure that our authority continues to operate effectively and securely. The safety and the integrity of our services and data are our top priorities, and strong cyber security is fundamental to achieving this.

6. We will do this by using Central Government's Cyber Security Framework ensuring we appropriately manage risk, protect ourselves from attack, prevent through detection and have suitably robust and expedient plans in place to minimise impact of any incident should it occur.

7. The Cyber Security Strategy will sit within the Technology & Digital Strategy

Framework underpinned by a library of policies created to ensure our staff follow the necessary practices in their duties. It places the responsibility on everyone in the organisation to ensure they actively participate in safeguarding our digital infrastructure, services and data.

8. Working with our Shared Technology Services Partner (STS), we are adopting the National Cyber Security Centre (NCSC) Cyber Assessment Framework (CAF) as our assurance framework.

9. The Ministry of Housing, Communities and Local Government (MHCLG) have been working with a small cohort of councils, which has included Southwark, to explore how local authorities should use the NCSC's CAF to assess and improve their cyber resilience and as the standard way of assessing cyber risk before the commencement of a nationwide rollout.

10. Southwark opted to volunteer for inclusion within this group as early adopters and support ongoing shared learnings that will go on to assist other UK councils, and therefore improving the broader support network in our sector.

11. The framework consists of a set of 14 cyber security and resilience principles, aimed at helping organisations achieve and demonstrate an appropriate level of cyber resilience.

12. The principles define a set of top-level outcomes that describe good cyber security functions, centred on four objectives. Each principle is accompanied by a guidance for achieving the outcome and recommends some ways to tackle common cyber security challenges.

13. Southwark and MHCLG have worked together on completing a CAF-lite version.

14. The final version is due for submission in the week commencing 4 November 2024, and we will hear the outcome later this year.

15. This is not a pass or fail exercise, but it will however provide further independent analysis of the efficacy of aspects relating to cyber security and what gaps and/or ongoing improvements could be addressed.

16. Alongside the internal and external audits and participation in the MHCLG CAF-lite, Technology Digital Services have also commenced a self-assessment of the full NCSC CAF, expected to conclude mid-November.

17. In doing so, this provides us with the following:
    - Baseline of our current position
    - Understand our risk profile
    - A plan to create a mitigating set of actions for each risk, which may include but not limited to;
        - implementation of or, changes to, policies and procedures
        - investment in security related tooling, people and/or replacement technologies
    - Staff training programme to educate and reinforce expected ways of working

- Appropriate governance forums to monitor open risks, cyclically re-assessed through the Audit workplan, CAF self-audits and assessments
- Continual learnings from our findings, implementing additional measures and/or recommend improvements to improve our security posture

18. These findings tie into the ongoing management of the organisational operating landscape and IT architecture that are monitored, updated through new controls and governance, tooling investment, technology replacement programmes and staff engagement programmes in order to continually improve our security posture and decrease our risk exposure.

19. Items arising from the CAF Assessment, audits and business as usual (BAU) operational monitoring are added to a security risk register, which is a standing agenda item continually reviewed at the Information Governance and Security Group chaired by Head of Technology & Transformation within Southwark and involves, where appropriate, the council's IT providers and suppliers, which meets fortnightly. This forum was formed over the summer.

20. At the SIRO Board, which meets quarterly, chaired by Strategic Director of Resources, attended by Southwark's Chief Digital & Technology Officer and STS Head of Cyber Security to report on new and progress of existing cyber risks, alongside other operational Information and Data security matters.

21. A council Cyber Security Strategy has been developed, currently under review by key stakeholder groups across the council and with STS for final comments. STS & partner organisations Joint Management Board (JMB) have, as of October, formed a cyber working committee that meets monthly. This is in addition to the daily operational functions and associated forums.

22. All compiled outputs and findings form part of the council's ongoing plan to improve our security posture which is owned by TDS, and are delivered through a number of workstreams:
    - Contract and relationship management of our supply chain (including STS)
    - Ongoing operational monitoring, management and remediation across all aspects of our IT Service Management and Enterprise Architecture
    - Implementation of the IT Project and Programme Portfolio
    - Implementation of the Council workplan
    - Implementation and ongoing monitoring and management of staff awareness and requisite training

23. Whilst our process and people aspects are maturing and our technology investment and future project workplan has laid strong foundations and only continues to strengthen our position, there is still a areas to be developed.

24. A brief overview of these activities, are listed below:
    Asset Management
    - LBS now have a dedicated resource in place working with STS tackling process improvements and recovery of end-user devices.
    - This has already led to £30k licensing saving through reclamation
    - Further education of staff around asset returns whereby managers hold on to devices for new starters to begin imminently

- Commencement of reporting through DMT's of non-returned assets within their directorates will commence later in the year

KEY ISSUES FOR CONSIDERATION

Recommendation: (1) Excessive Number of Domain Admin Accounts
Status: Completed – On-going Monitoring

25. Update**:** Admin accounts have been reviewed and updated in line with BDO recommendations.

26. The Information Governance and Security Group (IGSG) has created a document titled Periodic Governance Checks. This contains a list of all periodic governance actions required along with details. Regular audit of domain admin accounts added to this document. The review period, responsibility, and date of last review are recorded.

27. Monthly audit of all domain admin accounts now presented to the Operational Management Group meeting (OMG), attended by TDS and STS.

28. Incident Response (IR) team contacted with directions to update IR plan and run an IR scenario for a breach of a domain admin account. Date to be confirmed.

29. We have with STS reduced the number of days for account deactivation.

BDO Recommendation: (2) Non-Compliance with Anti-virus
Status: Completed – On-going Monitoring

30. Update**:** Regular audits to be conducted of all laptops not accessed for >90 days to deactivate such devices (work scheduled in Periodic Governance Checks document).

31. The reconciliation of devices is now scheduled and recorded in the Periodic Governance Checks document. Process overseen by Information Governance and Security Group.

32. Continuous check done on Anti-Virus status on laptops and servers done by STS. STS AV console also provides details of laptops that are not up to date with AV.

33. Procurement in progress to replace laptop estate and manage through newly implemented Microsoft InTune service. This will provide greater control over devices in terms of Anti-Virus, patching and configuration profiles for users.

34. Migration is due to start in December 2024.

BDO Recommendation: (3) Cyber-security e-learning compliance
Status: Implemented - On-going process

35. Update**:** Mimecast training has been rolled out since September 2024. Three videos selected as required training each month to ensure the training is more

accessible to staff. Cyber training was mandatory, but completion was difficult to track. Initial uptake of training has increased by 12 per cent to 62. The goal is to ensure all staff who use technology will complete the training.

36. Mimecast is now linked to Active Directory, providing the ability to track completion by staff member and Department, working with the council's Digital Learning team on tracking training performance.

37. Ongoing communication with business leaders is needed to drive awareness of training. Current focus: passwords (in coordination with new password policy and password refresh project), phishing and data protection.

BDO Recommendation: (4) Regular phishing exercise
Status: Implemented - On-going process

38. Update**:** The phishing campaign is in the planning stage, utilising Mimecast. The initial phishing test emails were distributed to members of the technical team.

39. We are engaging with HR and Unions ahead of a widespread phishing campaign due to start in November. A landing page has been created for users who click on phishing emails with information on how to spot phishing emails.

40. Frequently Asked Questions (FAQs) with answers provided to the Service Desk for users who contact the service desk following clicking on a phishing email.

41. Mimecast allows for tracking of who has completed the training. Working with the council's Digital Learning team to track training performance across the council.

BDO Recommendation: (5) Cyber Incident Response (IR) plan
Status: Completed - On-going Monitoring

42. Update**:** The Council held a Cyber Exercise on Dec 2023, in conjunction with the LBS Emergency Planning (EP) team, and a second event was held in July. Responsibility for the scheduling of these events lies with the EP team.

43. In addition, a Resiliency workshop was held in July with Brent, Lewisham and the shared service to identify Tier 1 applications / services and review resiliency capabilities. Follow up workshop to be scheduled in November.

44. The Council has numerous communication channels and key stakeholder groups to initiate a response in any event of a Cyber Incident. There is also a Data Protection document in development as part of the IR planning.

45. With the shared service we created a Cyber Role RACI model (Responsible, Accountable, Consulted, and Informed) which has now been completed. Emergency Planning has its own set of roles and responsibilities for business planning.

BDO Recommendation: (6) Network Access Control (NAC)
Status: In progress - Solution design in progress

46. Update**:** Completed a review and identification of open network ports as part of recent penetration testing exercise.

47. Should any unknown device attach itself to the LAN, it is put into remediation, and then asked for authentication via a certificate held on the device. A certificate can only be granted having followed the implemented process.

48. The Wi-Fi access is via Govroam and is authenticated and certificated access – meaning only verified users and their devices can connect. The public Wi-Fi access is outbound via the Public Internet only and unconnected to the council.

49. Proposals received for Network Access Control (NAC) solutions are currently being reviewed for selection. Once selected and implemented this will provide greater levels of security and resilience.

BDO Recommendation: (7) Cyber Security policy
Status: Policies written / in development

50. Update**:** Policies which have been written and published:
    - Acceptable Use Policy
    - Password Policy
    - Software Application and SaaS Policy
    - Privileged Access Management Policy
    - Hardware Asset Management Policy

51. The shared service and our partner councils (Brent, Lewisham) are working on additional policies.

52. In addition, a Cyber Security Risk Register has been developed for Southwark. This is reviewed as part of the Information Governance and Security Group's responsibilities.

BDO Recommendation: (8) Admin Account Policy
Status: In implementation - On-going Monitoring

53. Update**:** Privileged Access Management policy and Password policy documents written, approved, and published on the intranet.

54. The privileged access management policy was reviewed by the Technical Design Authority (TDA). A review of admin passwords and holders with the shared service. (see section above – **Admin Accounts**).

55. A review of Microsoft Configuration changes recommended by BDO is in progress.

Policy framework implications

56. N.A.

Community, equalities (including socio-economic) and health impacts

Community impact statement

57. N/A.

Equalities (including socio-economic) impact statement

58. N/A.

Health impact statement

59. N/A.

Climate change implications

60. As part of our commitment to environmental sustainability, our digital strategy is designed to align with the principles of responsible and eco-conscious technology management.

61. Our digital initiatives prioritise energy efficiency, emphasising the adoption of green IT practices such as Cloud utilisation, and reduction of printing.

62. We recognise the role of remote work and digital collaboration in reducing the need for physical travel, thereby contributing to lower carbon emissions.

63. Our technology and digital strategy also emphasises responsible product lifecycle management, considering the environmental impact of our technology choices from procurement to end-of-life. We are committed to minimising electronic waste through recycling programmes within the local area.

Resource implications

64. None. Appropriate skills and capacity is managed accordingly within the operational budget.

Note: Legal/Financial implications (and when to seek supplementary advice)

65. None. However the actions taken to meet the findings of the BDO audit help strengthen our approach to continue to comply with legislative requirements around GDPR and Data Protection.

Consultation

66. N/A.

SUPPLEMENTARY ADVICE FROM OTHER OFFICERS

Assistant Chief Executive, Governance and Assurance

67. N/A.

Strategic Director, Finance

68. N/A.

BACKGROUND DOCUMENTS

Background Papers	Held At	Contact
F-IT07 - Cyber Security review- FINAL Internal Audit Report	Internal Audit	Aaron Winter Aaron.winter@bdo.co.uk
2024- Nov Cyber Update AGSC - BDO Audit - final	Internal Audit	Aaron Winter Aaron.winter@bdo.co.uk

APPENDICES

No.	Title
Appendix 1	N/A

AUDIT TRAIL

Lead Officer	Dionne Lowndes		
Report Author	Dionne Lowndes		
Version	Final		
Dated	1 November 2024		
Key Decision?	No		
CONSULTATION WITH OTHER OFFICERS / DIRECTORATES / CABINET MEMBER			
Officer Title		**Comments Sought**	**Comments Included**
Assistant Chief Executive, Governance and Assurance		No	No
Strategic Director, Finance		Yes	Yes
Cabinet Member		Yes	Yes
Date final report sent to Constitutional Team			4 November 2024