LONDON BOROUGH OF CAMDEN

WARDS:

All

REPORT TITLE

Risk Deep Dive: Cyber and Data Security

REPORT OF

Executive Director of Corporate Services

FOR SUBMISSION TO

Audit and Corporate Governance Committee

DATE

21st January 2026

SUMMARY OF REPORT

This report provides Members with an overview of this principal risk to enhance the Committee's understanding of how this risk is being managed. The purpose of the risk deep-dive is to enable the Committee to fulfil its duties regarding monitoring the Council's effective operation of risk management as set out in its Terms of Reference.

Local Government Act 1972 – Access to Information

No documents that require listing have been used in the preparation of this report.

Contact Officer:

Andy Snape
Head of Technology
5 Pancras Square
London
N1C 4AG

Telephone: 020 7974 3738
Email: andy.snape@camden.gov.uk

RECOMMENDATIONS

Committee members are asked to note and comment on how this risk is being managed.

Signed: KMyers

Kathryn Myers, Interim Executive Director of Corporate Services

Date: 27 Jan 2026

1. Purpose of Report

1.1. In accordance with its Terms of Reference, the Audit and Corporate Governance Committee (the Committee) is required to monitor the Council's effective development and operation of risk management. In addition to this, the CIPFA position statement on Audit Committees in Local Authorities specifies several core responsibilities for audit committees, one of which is to "consider the effectiveness of the authority's risk management arrangements and the control environment."

1.2. The purpose of this risk deep dive is to allow the committee to obtain a deeper understanding of the Council's cyber security risks and to develop insight into the risk treatment plan.

2. Cyber security risk context

2.1. The cyber security risk environment facing the UK public sector continues to intensify, with local government remaining a high-value and persistent target. Councils hold large volumes of sensitive personal data, deliver critical statutory services, and often operate complex technology estates that include legacy systems. This combination increases exposure to ransomware, data exfiltration, denial-of-service attacks, and supply-chain compromise. Threat actors are increasingly sophisticated, well-resourced, and opportunistic, actively exploiting vulnerabilities, misconfigurations, and human factors such as phishing and credential theft.

2.2. Recent incidents across London boroughs underline the scale and impact of this risk. The cyber attack affecting the shared technology environment supporting Royal Borough of Kensington and Chelsea, Westminster City Council, and London Borough of Hammersmith and Fulham in November has had a prolonged and material operational impact. Several months on, services continue to experience disruption, with recovery activity extending well beyond immediate system restoration into data reconciliation, security re-engineering, and assurance work. This incident has demonstrated that cyber attacks are no longer short-lived technical events, but major organisational incidents with sustained consequences for service delivery, financial resilience, staff capacity, and public confidence.

2.3. The ongoing recovery from this incident also highlights wider sector challenges, including inter-dependencies created by shared platforms, third-party suppliers, and collaborative service models. While these arrangements can deliver efficiencies and consistency, they can also amplify the blast radius of a successful attack. For local authorities, this reinforces the importance of defence-in-depth, rigorous supplier assurance, management of legacy technology, and regular exercising of incident response and business continuity arrangements. It also emphasises the need for sustained investment in cyber maturity, rather than reliance on point-in-time compliance.

2.4. In this context, Camden's cyber risk should be viewed as part of a national and sector-wide threat landscape that is increasing in both likelihood and potential impact. Even with strong controls in place, the risk cannot be eliminated. The focus therefore remains on reducing exposure, improving detection and response capability, and ensuring organisational readiness to manage and recover from a serious cyber incident while continuing to protect residents and critical services.

2.5. Senior Officers within Camden's Customer, Technology & Data Services (CTDS) Division have consistently identified cyber security as one of the Council's highest-rated corporate risks in the Principal Risk Register. The assessed likelihood of a significant incident is scored at 3 out of 5, indicating that an incident is expected to occur in some circumstances and has been experienced elsewhere in the sector, with an estimated probability of around 20%. The assessed impact is scored at 5 out of 5, reflecting the potential for severe consequences, including financial losses in excess of £10m, prolonged disruption to critical services, and significant reputational damage to the Council.

2.6. The Council's approach reflects a low tolerance for cyber risk affecting critical services and personal data, while recognising that residual risk cannot be fully eliminated.

3. Overview of Camden's Cyber Security capability

3.1. Since April 2021, Camden has made sustained and deliberate investment in building a strong and mature cyber security capability. The function is led by an experienced Information Security Manager and supported by a dedicated team of nine information and cyber security professionals. Together, they provide strategic leadership and operational assurance, reflecting the critical role cyber security plays in protecting the Council's services, data, and residents.

3.2. Three officers within the team focus specifically on governance, risk, and compliance (GRC). Their work centres on operating an Information Security Management System (ISMS), which is the structured framework of policies, processes, and controls used to manage information security risks consistently across the organisation. This includes maintaining compliance with recognised public sector and industry standards, including the Public Services Network (PSN), the Payment Card Industry Data Security Standard (PCI-DSS), and the Cyber Assessment Framework (CAF). Over 50% of this team's time is spent managing supply-chain cyber risk. This reflects the Council's reliance on third-party technology suppliers and the fact that weaknesses in supplier security can present a direct risk to Camden. Structured security assessments are therefore carried out to identify, assess, and manage these risks before and during the delivery of services.

3.3. In parallel, Camden's security operations team is responsible for implementing technical security controls and for the ongoing monitoring of systems and networks. The team operates a modern suite of security tools designed to prevent attacks, detect threats early, and support rapid response where issues arise. Their work focuses on automation, investigation of suspicious activity, continuous improvement of Camden's security posture, and close involvement in major technology programmes. This ensures that security is embedded into new systems and that the Council's attack surface, meaning the number of potential entry points for attackers, is kept as small as possible.

3.4. Camden actively collaborates with peers across London through membership of Information Security for London (ISfL). Through this forum, councils are working collectively towards a more consistent and agreed cyber security baseline. Establishing a shared baseline is important to provide assurance that partners have appropriate controls in place, to reduce the risk of cross-organisational incidents, and to enable confident data sharing in support of joined-up public services. This collaboration also enables the timely sharing of lessons learned from cyber incidents affecting individual boroughs, helping to strengthen resilience across the public sector as a whole.

3.5. A common baseline would help reduce duplication of assurance activity and overall workload by providing greater confidence in partner controls. However, recent cyber incidents demonstrate that this level of consistency has not yet been achieved across the sector. As a result, Camden must continue to retain responsibility for its own cyber risk assessment and decision-making. Through ISfL, Camden is contributing to longer-term improvements in sector resilience, while ensuring that current partnership arrangements and data sharing decisions remain aligned to the Council's own risk appetite and service responsibilities.

3.6. The sections that follow provide more detailed information on specific cyber risks, controls, and improvement activity. This overview is intended to set the context and demonstrate that cyber security is an established and embedded capability within the Council.

4. Building a culture of information security

4.1. Building a strong culture of information security is a core part of Camden's approach to managing cyber risk. Information security is treated as a shared responsibility for everyone working for, or on behalf of, the Council, rather than as a purely technical issue. This was clearly demonstrated through recent peer review activity, which highlighted strong leadership ownership and organisational awareness. Camden's Chief Executive and the Corporate Management Team (CMT) have a clear understanding of the importance of cyber security, the risks the Council faces, and the potential impact on services and residents. They have consistently prioritised and supported the investment and culture change required to embed good security practices across the organisation.

4.2. A key pillar of this cultural approach is Camden's cyber awareness and training programme, underpinned by Hoxhunt. Hoxhunt is used to deliver regular, realistic phishing simulations to all officers and Members, helping to reinforce good security behaviours in day-to-day work. When a phishing email is correctly reported, users receive short, targeted training that explains what to look for and why it matters. This approach focuses on learning rather than blame and supports continuous improvement. Engagement levels are strong, with around 60% of users actively participating, and work is underway to link Hoxhunt participation more closely to Camden's mandatory training framework to further increase reach and consistency across the organisation. This activity is reinforced each October through dedicated events, communications, and engagement sessions delivered as part of Cyber Security Awareness Month, helping to refresh key messages, promote good practice, and maintain visibility of cyber risk.

4.3. Working in partnership with the Data Protection Team and Adults' and Children's Services, targeted technical controls have been introduced to reduce the risk of data breaches in high-risk social care environments. This includes the development of a custom dictionary of terms commonly used in social care practice, combined with real-time email controls that prompt practitioners to check the distribution list and the appropriateness of sharing sensitive information. Practitioners are required to actively confirm that these checks have been completed before information is sent, reinforcing accountability and professional judgement at the point of use. Since implementation, the number of reported data breaches has reduced significantly, providing clear evidence that combining awareness, process change, and technical controls can materially reduce risk.

4.4. Beyond the core workforce, Camden has extended its cultural focus into education settings. During Q4 2025, cyber security awareness training was delivered to staff and students in eight Camden secondary schools. This included the rollout of Hoxhunt to school staff, strengthening awareness in environments that hold sensitive data and rely heavily on digital systems. This activity was delivered with support from partners through the CTDS social value programme and achieved at no cost to the Council, demonstrating how social value can directly support cyber resilience.

4.5. CTDS has worked closely with the corporate procurement team to embed cyber security expectations into procurement processes. This includes integrating proportionate but robust cyber security assessments into specifications and supplier selection, ensuring that cyber risk is considered early rather than retrospectively once services are live.

5. Our approach to governance and risk management

5.1 Camden manages its cyber security governance and risk activity through a structured Information Security Management System (ISMS), supported by the use of ISMS Online. This tool enables the Council to record, track, and manage identified cyber security risks in a consistent and auditable way. We have a clear understanding of the key cyber risks affecting our most critical line-of-business systems and services. Work is ongoing to expand this coverage further, although the scale and complexity of the Council's technology estate means that building and maintaining a complete, real-time picture of all risks remains challenging.

5.2 To strengthen assurance and compensate for this complexity, Camden operates a regular programme of independent technical testing. This includes quarterly external penetration testing, which involves accredited specialists simulating real-world cyber attacks from outside the organisation to identify weaknesses before they can be exploited. In addition, Camden undertakes an annual IT Health Check, which includes internal penetration testing designed to assess risks from within the network, such as compromised user accounts or misconfigured systems. The most recent IT Health Check was completed in November 2025, and technical teams are currently working through the resulting remediation actions. These audit and remediation cycles have proven highly effective in improving the Council's overall security posture.

5.3 At a corporate level, the most significant cyber risks are reported through the Council's Principal Risk Register. However, there is an inherent balance to be struck between transparency and security. Publishing detailed technical vulnerabilities or system-specific risks would materially increase the Council's exposure to threat actors. As a result, reporting focuses on high-level risk themes, impacts, and mitigations rather than operational detail. Oversight of the ISMS is provided through annual review by the Corporate Information Governance Group (CIGG), which assesses its effectiveness and ensures that cyber risk management remains aligned with corporate governance arrangements.

6. Managing supply chain risks

6.1. Managing cyber risk across Camden's supply chain has become an increasingly significant area of activity and now consumes a substantial proportion of governance, risk, and compliance (GRC) capacity. The number of supplier security assessments required to support CTDS-led programmes and wider Council activity continues to rise year on year. In response, Camden has streamlined and standardised its assessment approach and moved to an online management tool in 2025 to improve efficiency, consistency, and auditability. Despite these improvements, overall workload has continued to grow as the Council's reliance on third-party digital services increases.

6.2. This growth is reflected in assessment volumes. In 2025, Camden completed 80 supplier cyber security assessments, compared to 53 in 2024 and 20 in 2023. These assessments are critical in identifying weaknesses in supplier controls that could expose the Council to data loss, service disruption, or regulatory risk. They also support informed decision-making by ensuring that risks are understood and, where necessary, mitigated before systems are procured or services go live. The rising volume of work highlights both the scale of third-party dependency across the Council and the importance of maintaining a robust, proportionate approach to supplier assurance.

6.3. We are working to addressing historic risk where supplier relationships are in place without the necessary contractual cyber security protections. Some legacy contract arrangements do not include appropriate security clauses, assurance rights, or incident notification requirements, increasing the Council's exposure and placing additional demand on our technical officers. Addressing these gaps requires targeted effort, working closely with procurement, legal, and service owners to strengthen contractual positions over time, when opportunities arise.

7. Business continuity and incident management

7.1. The Council has undertaken a comprehensive review of all business continuity plans during 2024 and 2025, coordinated by the Emergency Planning Service. This work has focused on ensuring that all services have robust and practical arrangements in place to continue delivery in the event of a major incident, including a significant cyber event. Within this context, Customer, Technology & Data Services (CTDS) has consistently emphasised that recovery from a cyber incident must be carefully prioritised. In the event of an attack, system and service restoration would follow the agreed recovery order approved by the Corporate Resilience and Governance Group (CRAG), ensuring that critical and statutory services are restored first and that recovery activity aligns with wider corporate priorities.

7.2. To support effective response and recovery, Camden has a retained cyber incident response service in place with an NCSC accredited supplier. This arrangement provides access to specialist incident response expertise in the event of a cyber attack, including technical containment, investigation, and recovery support. It also enables Camden to draw on expert consultancy to strengthen preparedness and improve response capability outside of live incidents. This provision has now been extended to the 47 schools taking the Council's Schools IT Support Service (SitSS) SLA, improving resilience and consistency of response across the education estate.

7.3. CTDS maintains a formal cyber incident response plan, which sets out clear roles, escalation routes, and decision-making arrangements during a cyber incident. This plan is tested every six months through externally facilitated desktop exercises to ensure it remains effective and well understood by senior officers and responders. The most recent exercise took place in September 2025, with the next scheduled for February 2026. This exercise has been brought forward in light of recent high-profile cyber incidents affecting London boroughs, reinforcing Camden's focus on learning from sector experience and maintaining a high level of operational readiness.

8. Disaster recovery

8.1. Customer, Technology & Data Services (CTDS) maintains a robust backup and recovery capability to protect Council data and support recovery from a major incident. This includes an immutable backup platform, which backs up all data stored on the Council's on-premise systems. Immutable backups are designed so that data cannot be altered, deleted, or encrypted once it has been written, even by an attacker. This provides strong protection against ransomware and malicious activity. The platform has been in use since June 2021 and will shortly be re-contracted. Cloud-based systems used by the Council include backup and recovery capabilities as part of their services and are not currently backed up through Rubrik. As part of the upcoming procurement exercise, CTDS will explore whether extending backup coverage to selected cloud services, such as Microsoft 365, would provide additional assurance and reduce recovery times, although this is expected to be cost-prohibitive.

8.2. While Camden has a high level of assurance that data is protected and can be restored, a key residual risk relates to recovery time. The Council's technology environment is large and complex, and although data loss is unlikely, restoring systems and services following a significant cyber incident could take a considerable period of time. This reinforces the importance of clear recovery priorities, strong coordination with business continuity arrangements, and realistic expectations around the pace of recovery following a major incident.

8.3. To support effective recovery, CTDS maintains detailed recovery runbooks for critical infrastructure and the top 20 critical line-of-business systems. These runbooks set out the agreed steps, dependencies, and responsibilities required to restore services in a controlled and safe manner. Looking ahead, CTDS plans to allocate dedicated resources to further recovery testing in Q4 2026 to strengthen assurance in this area, validate recovery assumptions, and identify opportunities to reduce recovery times by leveraging automation.

9. Joiners, movers and leavers processes

9.1. As part of this wider defence in depth strategy, CTDS has worked with the People & Inclusion Division to deliver a substantial redesign of Joiners, Movers and Leavers processes to strengthen identity and access management. This work ensures the Council has a clear and accurate understanding of who works for Camden, what systems they have access to, and why that access is required. Access is increasingly governed through role-based access controls, ensuring officers receive access aligned to their role and responsibilities and no more than is necessary. Changes in role trigger formal access review, and access is removed promptly and consistently when individuals leave the organisation. This reduces the risk of unauthorised or inappropriate access and underpins many of the technical controls described above.

10. Technical controls

10.1. Over the past four years, Customer, Technology & Data Services (CTDS) has pursued a defence in depth approach as part of a sustained programme to review, modernise, and secure the Council's IT environment. Defence in depth means applying multiple layers of protection so that if one control fails, others continue to reduce risk. This work has included the implementation of several modern cyber security tools, alongside improvements to core technical controls, with a strong emphasis on automation to support the timely detection, analysis, and response to security events.

11. Outlook for the next 12 months

11.1. Over the next 12 months, Camden's cyber security focus will continue to strengthen resilience, improve assurance, and reduce specific areas of exposure. However, the Council's overall cyber risk profile is not expected to reduce. This reflects an external threat landscape that continues to intensify, with increasingly capable attackers, greater automation, and sustained targeting of public sector organisations. At the same time, the Council's reliance on digital systems continues to grow as more services, data, and operational processes depend on technology.

11.2. Even with continued improvement in controls and capability, cyber risk cannot be eliminated and must be actively managed.

11.3. In this context, Camden must continue to focus on managing and mitigating cyber risk rather than seeking to eliminate it entirely. This includes maintaining strong organisational awareness through ongoing training for members, officers, and key partners, reinforcing individual accountability for information security, and ensuring that robust incident response and recovery arrangements are in place and ready to be activated when required. Preparedness, speed of response, and the ability to recover services safely remain as important as preventative controls.

11.4. From a governance and assurance perspective, Camden also anticipates increased expectations from central government in relation to cyber security maturity and assurance. It is increasingly likely that local authorities will be expected to demonstrate full compliance with the Cyber Assurance Framework (CAF) published by the National Cyber Security Centre. Camden has strong foundations in place through its established Information Security Management System (ISMS), which provides a structured and embedded approach to managing cyber risk. However, moving to full CAF alignment will require significant additional work, particularly in strengthening evidence, demonstrating control effectiveness, and extending assurance across the full technology estate and supply chain. This will further increase demand on governance, risk, and compliance (GRC) capacity.

11.5. In recognition of this sustained growth in workload, and the increasing complexity of the assurance landscape, CTDS plans to increase headcount within the GRC team by one additional role. This investment is intended to ensure that cyber risk continues to be managed proactively, proportionately, and in line with emerging central government expectations, while maintaining the resilience and effectiveness of the wider cyber security function.

12. Comments of the Director of Finance

12.1. The Director of Finance has been consulted and has no comments to add.

13. Legal Comments of the Borough Solicitor

13.1 The Borough Solicitor has been consulted in relation to the report and has no further comments to add.

14. Environmental Implications

14.1. There are no direct environmental impacts to highlight in this report.

15. Appendices

Appendix 1: Risk Deep Dive: Cyber and Data Security Control Details and Technical Roadmap (exempt)

Appendix 2: Principal Risk information and action plan (‘risk on a page’)

Appendix 3: Technical glossary

REPORT ENDS