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

Notes:

The likelihood score was reduced from 4/5 to 3/5 in October 2024 to reflect improvements in preventative and detective controls, while recognising that the overall cyber threat facing the local government sector remains high. Given the increasingly hostile and dynamic threat landscape, CTDS will recommend that the likelihood score be reverted to 4/5 at the next review of the Principal Risk Register.

The target score reflects strengthened containment, response, and recovery capability, rather than a reduction in the underlying cyber threat.

<table>
<tr><th colspan="3">Cyber and Data Security</th><th>Existing Controls</th></tr>
<tr><td><b>Current Score: 15</b> (L:3, I:5)</td><td><b>Target Score: 9</b> (L:3, I:3)</td><td><b>Outlook</b>: Increasing</td><td rowspan="2">1. Data, digital and technology policy and controls in place, such as device encryption, email security, role-based access controls, web access firewall (C-WAF), Endpoint Detection & Response (EDR).
2. Corporate Induction training regarding computer usage policy and information security policies.
3. Quarterly party penetration testing to test and improve our data, digital, and technology security.
4. Compliance and statutory standards projects
5. Cross-council coordination to remove users from systems when they leave.
6. Robust standards for authentication and integrated security monitoring.
7. Business Continuity and Disaster Recovery Plans
8. Six-monthly desktop exercises testing the Cyber Incident Response Plan
9. Monthly system updates and reporting.
10. Digital Services continue to be involved in the procurement process to improve cyber security. Robust security assessments provide assurance on all technology suppliers.
11. Internal Communications and ongoing awareness training programmes for all staff focus on behavioural change.
12. Contract in place with cyber incident response partner.</td></tr>
<tr><td colspan="3"><b>Risk:</b> Process control networks, devices and/or critical information assets/data may be compromised
<b>Cause:</b> Computer-based unauthorised access, denial of service, and malicious modification of code or unknown damage/access. End of life/aging Information Technology (IT) kit and infrastructure
<b>Consequence:</b> Potential loss of access to all systems and data, limiting our ability to deliver services and business as usual. Potential compromise to our access to data either temporarily or permanently (including historical case data). Damage, restricted access, denial of access, denial of service or information breach.
<b>Risk Update:</b>
The overall cyber threat landscape remains complex and ever-changing, with increasingly sophisticated tools and attack methods employed against organisations. The Customer, Technology & Data Services (CTDS) division has continued to deliver critical work as part of the Council’s Cyber Security Programme, including maintaining higher-risk legacy systems. We have successfully recertified as compliant with the Public Service Network (PSN) standard and Payment Card Industry Data Security Standard (PCI-DSS), and a continued focus on security remediation with targeted activity based on severity, leveraging our vulnerability management platform. Our programme to remediate security vulnerabilities in all 48 Camden schools taking the Schools IT Support Service (SitSS) SLA is now advanced. This work is being led by a Cyber Security Analyst dedicated to SitSS and follows detailed vulnerability scanning and risk assessments completed early in 2025. CTDS is delivering an extensive set of cyber awareness training to secondary school staff and students as part of the annual October Cyber Awareness Month.
CTDS staff continue to participate in externally facilitated desktop exercises to test the Council’s approach to a range of service-impacting incidents, and we are collaborating with the Emergency Planning service to further integrate and test this with the Councils incident management processes. We are in the process of re-procuring the cyber</td></tr>
</table>

incident response contract, which will be extended to cover schools, bringing the insurance offered by the Council in line with the DfE Risk Protection Arrangement (RPA). CTDS continues to focus on leveraging investments in modern technology; our skilled cyber team and continuing focus on processes and procedures as part of our Information Security Management System (ISMS) are improving overall organisational maturity in information governance. Finally, we are now planning phase two of our alignment with the new Cyber Assurance Framework (CAF) published by the National Cyber Security Centre (NCSC).	

Actions	Action owner	Status	Due Date	Risk owner
1. Deliver ongoing staff cyber training and awareness-raising.	1. A Snape	1. In progress	1. Ongoing	K Myers
2. Deliver the applications and infrastructure rationalisation and other priority programmes to eliminate or upgrade remaining legacy systems.	2. T Khan, A Snape and N Abraham	2. In progress	2. Ongoing	
3. Deliver ongoing Information Security Programme aligned to the Cyber Assurance Framework ensuring continuing risk-based approach to cyber security remediation.	3. A Snape	3. In progress	3. Ongoing	
4. Deliver the Schools (SitSS) Security Remediation Programme	4. A Snape	4. In progress	4. Mar 2026	

APPENDIX ENDS

Appendix 3: Technical glossary

Attack surface
The total number of ways a system or organisation could be attacked. This includes devices, applications, user accounts, and internet-facing services. Reducing the attack surface lowers overall risk.

Business Continuity Plan (BCP)
A plan that sets out how services will continue to operate during a major disruption. This includes cyber incidents, system outages, or loss of access to buildings or data.

Cyber Assurance Framework (CAF)
A framework published by the National Cyber Security Centre that defines what "good" cyber security looks like for public sector organisations. It focuses on outcomes, not just policies, and requires clear evidence of control effectiveness.

Cyber incident
An event where systems, data, or services are compromised or disrupted. This can include ransomware attacks, data breaches, or denial of service incidents.

Defence in depth
A security approach that uses multiple layers of protection rather than relying on a single control. If one layer fails, others continue to reduce the impact of an attack.

Endpoint
A device that connects to the Council's systems, such as a laptop, desktop computer, tablet, or mobile phone. Endpoints are a common target for cyber attacks.

External penetration testing
Controlled testing carried out by specialists who attempt to break into systems from outside the organisation. This helps identify weaknesses before real attackers can exploit them.

Governance, Risk and Compliance (GRC)
Activities that ensure cyber risks are identified, understood, and managed in line with legal, regulatory, and organisational requirements. This includes policies, assurance, and supplier assessments.

Immutable backup
A backup that cannot be altered, deleted, or encrypted once created. This protects data from ransomware and malicious activity and supports reliable recovery after an incident.

Information Security Management System (ISMS)
A structured set of policies, processes, and controls used to manage information security risks consistently across an organisation. It provides assurance that risks are identified and managed in a controlled way.

Internal penetration testing
Testing that simulates an attack from inside the organisation's network. This helps

assess what could happen if an attacker gained initial access, for example through a compromised user account.

Joiners, Movers and Leavers (JML)
Processes that control access when someone joins the organisation, changes role, or leaves. Strong JML controls ensure people only have access to systems they need, for as long as they need it.

Lateral movement
The ability of an attacker to move between systems after gaining initial access. Limiting lateral movement reduces the scale and impact of a cyber incident.

Legacy systems
Older technology that may no longer be fully supported or designed to meet modern security standards. Legacy systems often increase cyber risk and require additional mitigation.

Multi-Factor Authentication (MFA)
A security control that requires more than just a password to sign in. This usually includes something the user has, such as a code or app approval, making accounts much harder to compromise.

NEC Housing
A core Council system used to manage housing services, including tenancy information, repairs, and housing applications. It contains sensitive personal and financial data.

Network segmentation
The practice of separating parts of a computer network to limit how systems can connect to each other. This helps contain an attack if one system is compromised.

Penetration testing
A controlled exercise that tests how secure systems are by attempting to exploit weaknesses. Results are used to prioritise fixes and improve security.

Phishing
A type of cyber attack where fake emails or messages are used to trick users into revealing passwords or opening malicious links. Phishing is one of the most common causes of security incidents.

Principal Risk Register
The Council’s formal record of its most significant strategic risks. Cyber security appears here due to its potential impact on services, finances, and reputation.

Recovery runbook
A documented set of steps used to restore systems after an incident. Runbooks help ensure recovery is controlled, prioritised, and repeatable.

Role-based access control
A method of managing access where permissions are linked to job roles rather than individuals. This reduces the risk of excessive or inappropriate system access.

Security Information and Event Management (SIEM)
A system that collects and analyses security data from across the organisation. It helps identify suspicious activity and supports faster response to threats.

Single Sign-On (SSO)
A system that allows users to access multiple applications with one secure login. This improves usability while still enforcing strong security controls.

Supply chain cyber risk
The risk that a third-party supplier’s systems or practices could expose the Council to cyber attack. Managing this risk is essential due to reliance on external technology providers.

Technical debt
In legacy systems, technical debt is the build-up of outdated design choices, technologies, and shortcuts that make the system fragile, expensive to run, and difficult to change. It often locks organisations into old ways of working, where even small changes carry high risk and disproportionate effort.

Virtual Private Network (VPN)
A technology that creates a secure connection into an organisation’s internal network from outside locations. VPNs can increase risk if user accounts are compromised.

Zero Trust
A security approach that assumes no automatic trust anywhere in the network. Every user, device, and access request must be continuously verified, reducing the impact of breaches and supporting secure collaboration.

APPENDIX ENDS