APPENDIX A - CORPORATE SERVICES NET 'HIGH' RISKS

Ref:	**Risk Title and Description:**	
1	IT Security Failure	
Division:	**Risk Category:**	**Risk Owner:**
Corporate Services	Data and Information	Assistant Director - IT
Risk Cause and Effect:		
Cause(s): Failure of IT Security (responsibility across Bromley & BT) to manage risk of attack or intrusion leading to potential corruption / loss of data / loss of systems. Failure to comply with relevant legislation (GDPR) Failure to ensure the confidentiality, integrity, and availability of information assets. **Effect(s):** 1. Distress and/or physical impact on wellbeing of customers 2. Impact on operational integrity 3. Reputational damage to services and the authority as a whole 4. Liability in law 5. Economic damage to authority and/or customers 6. Impact on service take up due to reduced confidence from the public		
Gross Risk Rating:		
Likelihood	**Impact**	**Risk Rating**
4	**5**	**20**
Existing Controls in Place to Mitigate the Risk		
-Application of effective security management including effective application of anti-virus protection and security measures through the IT Contract with BT - Regular Penetration Testing undertaken - Information Security Team in place - Patch updates undertaken regularly - LBB is currently compliant with the Public Services Network Code of Connection (PSN CoCo), Cyber Essentials and DSP Toolkit and PCI-DSS (Payment Card Industry standards) The LBB Corporate Leadership Team formally accept the above certifications as the basis of LBB's internal information governance and security program. These standards are based on the ISO27001 international best practice and NCSC guidance for managing information security and are therefore fit for purpose for assessing and managing the Council's information risk - GDPR Training programme in place - Induction programme in place - Additional resources to manage riskd - Security Operation Centre (SOC) has been implemented which proactively monitors the LBB Data and Infrastructure.		

Current Risk Rating:

Likelihood	Impact	Risk Rating
3	5	15

Further Action Required:

- Review CIS benchmarking and secure score for On-prem, HCI and Azure servers. Implement CIS level 1 security patching

- Mature DLP tool to ensure false positives are tuned out and that policies capture and flag high risk email communication

- Ensure internal reporting of data breaches happens in a timely way

- Ensure that services are supporting the SAR processes in a timely way

Commentary from Risk Owner:

The Security Operation Centre (SOC) has been implemented which is being fine-tuned to ensure efficient proactive monitoring of the LBB Data and Infrastructure. Monthly reports are provided from the SOC setting out the top ten threats to the Council. These are being further developed to include information on which specific controls prevented these threats so that we can analyse whether compensating controls require strengthening.

The renewed BT contract strengthened the approach to proactive vulnerability management. The Council will have an external company conducting its annual IT Health Check in May, producing a report for actioning with BT. This will test the infrastructure configuration, penetration tests, residual vulnerabilities and device builds.

A new staff training package is being developed for 2024 for security and data protection which will be mandatory for all staff to complete.

The inherent risk will always be high because the threat is continually evolving and therefore keeping pace with the latest threats is an ongoing challenge. Whilst the Council has a number of controls in place, breach of any of these controls could result in a successful cyber attack.

Ref:	**Risk Title and Description:**	
16	Information Request non-Compliance	
Division:	**Risk Category:**	**Risk Owner:**
Corporate Services	Data and Information - Operational	Director of Corporate Services/ Assistant Director - IT
Risk Cause and Effect:		
Cause(s): Failure to meet timescales under FOIA, EIR and GDPR Failure to provide suitable answers in respect of these requests or correctly apply exemptions Effect(s): 1. Distress on wellbeing of customers 2. Impact on operational integrity 3. Reputational damage to services and the authority as a whole 4. Liability in law 5. Economic damage to authority due to fines		
Gross Risk Rating:		
Likelihood	**Impact**	**Risk Rating**
4	**5**	**20**
Existing Controls in Place to Mitigate the Risk		
SAR Team formed in the Information Management Team to ensure timely triage, collation, redaction and response. Appeal to COE, CLT, Manager's Briefing and all officers to support the information coordinators.		
Current Risk Rating:		
Likelihood	**Impact**	**Risk Rating**
4	**4**	**16**
Further Action Required:		
- Annual and increased training and awareness - experienced resources to triage and redact where necessary - improved technical measures to assist Data searches		
Commentary from Risk Owner:		
Annual and increased training and awareness - experienced resources to triage and redact where necessary - improve technical measures to assist Data searches including the possibility of direct access to key information systems, improved information management (storing files in the correct place, adhering to retention schedules, not using the mailbox as an information store) To improve compliance, there needs to be organisation-wide ownership of the Council's responsibilities under FOI, EIR and SAR and legislation. FOI and EIR responsibilities are devolved to individual departments.		

Monthly reports are presented to Corporate Leadership Team on FOIs, EIRs and SARs. These reports highlight requests outstanding and overdue and hotspots where there are high numbers of open and overdue FOIs.

FOI / SAR learning sessions have been run for any officer to attend and these will continue to be run – further promotion required from HR and department leads to encourage more staff to attend these awareness sessions.

Information Co-ordinators have been asked to undertake FOI training provided by the ICO.

Information Co-ordinator meetings will take place on a regular basis and proposed process improvements will be discussed at the next meeting in May.