Corporate Services Risk Register. Gross 'High' (Red) Risks Extract - Appendix A.

															DATE LAST REVIEWED:	06/05/2022
REF	DIVISION	RISK TITLE & DESCRIPTION (a line break - press alt & return - must be entered after the risk title)	RISK CAUSE & EFFECT	RISK CATEGORY	GROSS RISK RATING (See next tab for guidance)			EXISTING CONTROLS IN PLACE TO MITIGATE THE RISK	CURRENT RISK RATING (See next tab for guidance)			FURTHER ACTION REQUIRED	RISK OWNER
					LIKELIHOOD	IMPACT	RISK RATING		LIKELIHOOD	IMPACT	RISK RATING		
1	Corporate Services	**IT Security failure**	**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 **Effect(s):** Loss of service, potential fines, resident dissatisfaction	Data and Information	4	5	20	-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 - IG training programme - PSN Compliant	2	5	10		Vinit Shukle
2	Corporate Services	**Telecommunications failure** Prolonged telecoms / switchboard failure	**Cause(s):** Power surge, contractor failure, malicious attack, IT failure **Effect(s):** Widespread disruption across the Council	Data and Information	3	5	15	- Stand-by arrangements available so that in the event of failure highest priority services can be recovered - Technical design takes into account the criticality of systems and ensures, where justified, that additional resilience is built in - All Critical Services now have additional independent lines as contingency (if not their first line) - Additional resilience in use of LBB mobile phones - The ICT Disaster Recovery Plan is in progress - Working with BT to implement disaster recovery arrangements as part of new backup contract - Effective application of anti-virus protection and security measures through the IT contract with BT	2	3	6	- Virtualisation project will help facilitate disaster recovery provision - Secondary Session Initiation Protocol (SIP) connection being added to provide resilience.	Vinit Shukle
3	Corporate Services	**IT System Failure (partial loss)** Partial loss of IT systems	**Cause(s):** Failure of Outlook or similar applications Failure of Novell Filing Registry system which carries details of all departmental files **Effect(s):** Widespread disruption across the Council	Data and Information - Operational	4	4	16	- Effective incident management / support and resilient systems in use so that single points of failure are minimised - Technical design that takes into account the criticality of systems and ensures, where justified, that additional resilience is built in - Ensure proactive monitoring tools are in place to highlight potential issues before there is a major incident - System now migrated to the server - No longer dependent on Win7 - all services successfully transferred. However, the Novell filing registry/Regnet system has no further upgrade options and is not compatible with Win10 which will be deployed before December 2019 (Win7 support expiry date)	4	3	12	The Norwell System is currently used by legal team for historical file information only on a 'stand alone' PC. As part of any future platform upgrades, investigation will need to be carried out as to whether this option is still viable (by way of impact assessment) or look at migrating the historical data into Norwel (the current system).	Vinit Shukle
4	Corporate Services	**IT System Failure (total loss)** Complete failure of IT systems resulting in widespread disruption across the Council	**Cause(s):** Complete loss of data centre and related hardware **Effect(s):** Widespread disruption across the Council Financial loss Reputational impact	Data and Information - Operational	3	5	15	- Effective incident management / support and resilient systems in use so that single points of failure are minimised - Technical design that takes into account the criticality of systems and ensures, where justified, that additional resilience is built in - Ensure proactive monitoring tools are in place to highlight potential issues before there is a major incident - Backup power arrangements in the event of power issues (most likely) - Server room has fire suppression, water detection and significant physical security measures have been undertaken.	2	4	8	- Property are planning additional works to resolve the issues that caused the outages, but until then we remain at an elevated risk.	Vinit Shukle
8	Corporate Services	**Effective governance and management of information**	**Cause(s):** - Lack of organisational buy-in from information asset owners - Lack of governance - Poor awareness / education in understanding purpose **Effect(s):** - Breach of statutory obligations through failure of compliance with relevant legislation e.g. GDPR, UK DPA, FOIA, EIR - potential fines - increased information security attack surface - increased storage costs for on-prem data	Data and Information - Operational	4	4	16	- information governance training provided to all officers - system security reviews - SIEM system monitoring - Data Protection Impact Assessments	3	4	12	review and implementation of retention schedule in all systems hosting data	Vinit Shukle
9	Corporate Services	**Compliance with Information Request laws**	**Cause(s):** - Lack of organisational awareness - responsibility for responding are add on tasks to existing roles - data sprawl and lack of retention - large data scopes - lack of indexing and search capabilities **Effect(s):** - Breach of statutory obligations through failure of compliance with relevant legislation e.g. GDPR, UK DPA, FOIA, EIR - potential fines - reputational damage	Data and Information - Operational	4	5	20	- information governance training provided to all officers - system security reviews - SIEM system monitoring - Data Protection Impact Assessments	3	5	15	- increased training and awareness - experienced resources to triage and redact where necessary - improved technical measures to assist data searches	Vinit Shukle

Corporate Services Risk Register. Gross 'High' (Red) Risks Extract - Appendix A.

															DATE LAST REVIEWED:	**06/05/2022**
REF	**DIVISION**	**RISK TITLE & DESCRIPTION (a line break - press alt & return - must be entered after the risk title)**	**RISK CAUSE & EFFECT**	**RISK CATEGORY**	**GROSS RISK RATING** *(See next tab for guidance)*			**EXISTING CONTROLS IN PLACE TO MITIGATE THE RISK**	**CURRENT RISK RATING** *(See next tab for guidance)*			**FURTHER ACTION REQUIRED**	**RISK OWNER**		
					LIKELIHOOD	**IMPACT**	**RISK RATING**		**LIKELIHOOD**	**IMPACT**	**RISK RATING**				
12	Corporate Services	**Data Protection Breach**	**Cause(s):** Failure to adapt to the upcoming change in 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	Data and Information - Operational	4	5	20	- LBB is currently compliant with the Public Services Network Code of Connection (PSN CoCo) and Connecting for Health Information Governance Toolkit (CfH IGT). The LBB Information Governance Board formally accepted the CfH IGT as the basis of LBB's internal information governance program at their meeting in August 2012. Both standards are based on the ISO27001 international best practice standard 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 risk**	2	3	6		Director of Corporate Services	

Remember to consider current Internal Audit priority one recommendations when identifying, assessing and scoring risks.