Corporate Risk Register

Reported to: Audit and Governance Committee
Date: 27 June 2018

Ref	Details of Risk				Inherent Risk				Existing Controls	Residual Risk			Actions			
	Risk Description	Trigger	Result	Owner	Probability	Impact	Score		Existing Controls	Probability	Impact	Score	Proposed Action Plans	Action Owner	Target Date	Action Status
	A. CUSTOMER PERSPECTIVE															
	None															
	B. FINANCIAL & RESOURCES															
B1	Inadequate capability to prepare for and respond effectively to a major incident affecting the Council or occuring in Sefton.	A major incident occurs affecting the Council or the Borough. This risk is accentuated as the government has determined the terror threat level as "severe".	1) Loss of human life, illness or serious injury 2) Major damage or destruction to infrastructure, property and/or the environment 3) Disruption or loss of critical services such as transport, communications, utility services 4) Reputational or financial harm to the authority	SLB	4	5	20	Emergency Response Manual in place. Emergency Duty Co-ordinators invited to attend quarterly briefing sessions and all are able to access Resilience Direct containing incident response plans. Two senior managers have received Gold Commander training Attendance and participation in Merseyside Resilience Forum and joint planning across Merseyside is in place. Humanitarian volunteers in place and team strengthened following successful recruitment drive in February 2018. Plans for response and recovery are the subject of ongoing review and update, particularly in light of the government's assessment of the terror threat level as "severe".	4	4	16	Review of response and recovery has been undertaken with the objective of strengthening the current arrangements in the light of the terror threat level being at "severe" (and having been at critical for a short period); further to this review appropriate measures will be undertaken to strengthen operational capability in this area.	SLB	Aug-18	
B2	Dedicated Schools Grant High Needs Funding for Special Educational Needs is inadequate to meet requirements.	High Needs budgets are under considerable pressure from increasing numbers of children being diagnosed with complex and life-long SEND related issues. National funding allocations are not increasing annually to reflect increases in local population demand and so any additional commissioned places need to be financed from within existing budget envelope. The number of pupils needing High Needs top-up funding is increasing year on year, in-house provision is almost at full capacity and external provision is very expensive (3 or 4 time more expensive than in-house provision).	Overspending occurred in 2016/17 (£1.5m) and 2017/18 (£2m) and there is a chance of continued overspending in 2018/19 and beyond.	HoS&F	4	5	20	Engagement with Head of Schools and Families and the SEN team Managers on how costs can be contained. Engagement with special schools actively working with individual schools to review impact of any proposed changes to their funding, reviewing 3 year financial plans, identifying any strategic savings to mitigate high calls on DSG High Needs funding. Review of place and top up levels of funding to special schools to try to reduce costs. DfE has also provided each LA with additional grant funding to help provide additional capacity to undertake strategic needs assessment of SEN provision (£104k for Sefton) - this should help identify strategy to support cost pressure going forward.	4	5	20	The projected overspend on High Needs funding for 2017/18 will be contained within the DSG by using reserves. Schools Forum has agreed to move funding between the DSG funding blocks in 2018/19 to ensure the High Needs budget is balanced. Schools Forum have asked Officers to review SEND spend over the coming year with a view to reducing cost to within the allocated budget by 2019/20. Lobbying of Government continues with a view to securing increased funding. There is a review team plotting expected demand over the next 5-10 years, so as to provide clarity on likely future needs.	HoS&F	Ongoing	

	Details of Risk				Inherent Risk			Existing Controls	Residual Risk			Actions			
Ref	Risk Description	Trigger	Result	Owner	Probability	Impact	Score		Probability	Impact	Score	Proposed Action Plans	Action Owner	Target Date	Action Status
B3	Failure to adequately invest in the Highway Network and associated assets	Budget reductions; inadequate funding levels to meet need.	Deterioration of highway assets Potential increase in claims Financial and reputational risks Potential increase in accidents resulting in injury and/or death	SLB	4	5	20	Essential work is prioritised within available budget. Regular inspections of most assets to monitor and guide prioritisation of works in order to mitigate risk. Regular updates provided to Cabinet Member. Preventive surface treatments used to prolong the life of the network and to treat more of it than if more long-term maintenance solutions were used (ie resurfacing)	4	4	16	Reports submitted to Strategic Capital Infrastructure Group to seek additional funding to maintain or replace highway network/assets.	THI SM	Ongoing	
B4	Data Breach resulting in the wrongful release of personal and/or sensitive information	Policies and processes coordinated by Information Management and Governance Executive Group are not adhered to, resulting in a higher incidence of breaches caused by human error. System error occurs.	Failure to comply with legal requirements; loss of privacy, distress or harm to the data subject; damage to Council's reputation; loss of public confidence; and significant financial penalties.	SLB	4	5	20	Information Management & Governance, including data breaches and actions to prevent data breaches, is overseen by the Information Management & Governance Executive Group (IMGEG), which consists of Heads of Service with lead responsibilities for key aspects of IMG (ie designated Chief Information Officer, Senior Risk Information Officer and Lead officer for ICT infrastructure) supported by other officers with key roles relating to IMG. Each service has designated Information Asset Owners and Information Asset Administrators. Policies, procedures, processes and issues are communicated to these officers through the Information Management & Governance Tactical Group. Support, co-ordination, advice and guidance is provided corporately and appropriate training/refresher training is in place. The Council has implemented policies, procedures and processes to prevent, manage and respond to potential and actual data breaches.	4	5	20	Appropriate resourcing, prioritisation and focus on Information Management & Governance across the Council. Regular monitoring and review by IMGEG of policies, procedures and processes to prevent, manage and respond to potential and actual data breaches. Ongoing review of information systems to ensure no innapropriate or unforeseen data linkages exist within systems or reports. Review of systems ahead of updates to identify any unintended changes. Ongoing education of staff and monitoring of activity by IAOs and IAAs to identify and prevent areas of human error. Regular review of information contained to ensure information is accurate and any information that should be removed is removed. Regular reporting by IMGEG to SLB and Audit & Governance Committee as necessary. Maximise the opportunities from the Council's ICT Transformation to increase and embed effective information manangement and governance.	IMGEG	Ongoing	

		Details of Risk			Inherent Risk					Residual Risk			Actions			
Ref	Risk Description	Trigger	Result	Owner	Probability	Impact	Score	Existing Controls	Probability	Impact	Score	Proposed Action Plans	Action Owner	Target Date	Action Status
B5	Failure to correctly manage historic records	The risk is amplified by the implementation of GDPR (in particular the right to erasure and the tighter deadlines for response to Subject Access Requests) as well as the Council's Asset Maximisation programme which may lead the Council to leaving, redeveloping or selling buildings where records are held and moving to Paper Light working arrangements.	Failure to comply with legal requirements relating to retention, consideration, release or correct disposal of historical information; damage to Council's reputation; loss of public confidence; and significant financial penalties. Historical information is not stored or managed correctly, such that it is lost, damaged or incorrectly disposed of. Not known to the organisation when making relevant decisions; retained when it should have been correctly disposed of.	SLB	4	5	20	Information Management & Governance is overseen by the Information Management & Governance Executive Group (IMGEG), which consists of Heads of Service with lead responsibilities for key aspects of IMG (i.e. designated Chief Information Officer; Senior Risk Information Officer; and Lead officer for ICT infrastructure), supported by other officers with key roles relating to IMG. Each service has designated Information Asset Owners and Information Asset Administrators. Policies, procedures, processes and issues are communicated to these officers through the Information Management & Governance Tactical Group. Support, co-ordination, advice and guidance is provided corporately and appropriate training/refresher training is in place. The Council has implemented policies, procedures and processes for the management of information and has in place corporate contracts for appropriate digitisation, disposal and archive storage services. The Council has implemented a Historic Records Pilot Project to identify the scale, condition and correct management of all historic records held. This project reports regularly to IMGEG.	4	5	20	Appropriate resourcing, prioritisation and focus on Information Management & Governance across the Council, including support for Information Asset Owners and Information Asset Administrators. Regular monitoring and review by IMGEG of policies, procedures and processes for the management of information, including historic information. Regular monitoring and review by IMGEG of the progress and implications of the Historic Records Pilot Project, including reporting to SLB and Audit & Governance Committee as necessary. Maximise the opportunities from the Council's ICT Transformation to increase and embed effective information manangement and governance.	IMGEG	Ongoing	
B6	Failure to plan within annual budget for increased placement costs in Children's Social Care.	Numbers of children in care increases, demand for placements can not be met as cost of palcements increases.	Costs increase and quality and sufficiency of placements decreases. Budget overspend.	HoCSC	4	4	16	Fortnightly meeting to monitor placement costs. Programme of LAC reform including recruitment of in house carers. Development of Disability pathway. Development of market place. Annual Budget.	4	4	16	Development of market to meet need. Opportunities to collaborate across LCR and develop market. Regular review of budgets to identify and mitigate pressures. Introduction of placement panel.	HoCSC/ Service Managers/ Commissioning	Jun-18	
B7	Financial sustainability post 2020.	Government settlement places further strain on Council budget. Due to the scale of budget reductions since 2010 there is a risk that further suitable cost-saving/income generating measures will be difficult to identify.	Degradation of service Poor reputation Financial Sustainability could be compromised	SLB	5	5	25	Work ongoing to identify the Framework for Change post 2020. Horizon-scanning in place to identify funding trends and future service demand pressures.	4	4	16	Continuation of planning to identify the Framework for Change post 2020.	Dir SC&H	Ongoing	
B8	The Council is the victim of a cyber attack.	Malware, ransomware or another virus infects the Council's systems.	Services will not have access to systems and data as standard, and will have to fall back on non-ICT delivery methods, albeit without access to key data. Data breach occurs. Financial impact of ransom Reputational damage	HoCR	4	5	20	Cyberattack prevention measures are in place, including upgraded Council firewalls and active SIEM monitoring service. Back-up DR facility is in place at a separate site, allowing Arvato to restore the top 20 critical systems within 48 hours. Arvato has a BC-DR plan in place which covers an action plan for this priority restoration, and the subsequent restoration of all other systems. Ongoing monitoring in in place via ICT Working Group and FISOB. Sophos anti-virus software is constantly updated. Communication to employees regarding the rise in malware attacks is in place, with plans to roll out better user education on this topic.	4	4	16	The ongoing ICT Transformation programme will see the majority of systems and data migrated to Microsoft Azure cloud hosting, which will reduce the overall risk; however, consideration will be given to the risk profile of those services remaining on-premise following the completion of migration in August 2018. Review risk profile following completion of ICT Transformation programme. Implementation of user education re:malware. Develop new BC-DR plan following completion of ICT Transformation programme and appointment of new ICT services provider	HoCR	Ongoing	