Appendix 2

Strategic Risk Register as at 19 April 2019

***Ranked in order of Gross Risk**

				Current risk		
Ref	**Risk**	**Risk owner**	***Gross Risk**	**Likelihood**	**Impact**	**Score**
9 **(New)**	The implications of EU Exit potentially affecting the availability of Council's resources to deliver services which may impact on communities **(Assessment attached)**	CMT	16	Likely	Medium	12
10 **(New)**	The Council is hit by a Cyber-attack that compromises the confidentiality, integrity and availability of information and systems. **(Assessment attached)**	CMT	16	Moderate	High	12
1	Failure to address the financial gap in the Council's budget and achieve the target within the Medium-Term Financial Strategy resulting in non-achievement of Council strategic priority of Making Gateshead a Place Where Everyone Thrives.	CMT	16	Likely	Medium	12
2	Failure to manage demand and expectations could result in the Council not achieving its Thrive agenda.	CMT	16	Moderate	Medium	9
3	Failure to safeguard vulnerable children and adults	CMT	16	Unlikely	High	8
6	Failure to address workforce planning and resourcing requirements impacting on service delivery.	CMT	16	Moderate	Low	6
4	Failure to attract inward investment and deliver sustainable economic growth.	CMT	12	Moderate	Medium	9
5	Non-compliance with statutory requirements resulting in prosecution and subsequent penalties.	CMT	12	Likely	Low	8

7	Failure to provide a response during a Major incident or business interruption affecting availability of the Council's resources and impacting on ability to deliver critical services or an impact on a community.	CMT	8	Unlikely	Medium	6

New Assessments

Risk No	Risk Description	Risk Owner
9	**The implications of UK Exit from the EU potentially affecting the availability of Council's resources to deliver services which may impact on communities**	**Corporate Management Team**

Details of the risk	On the 14th of November 2018, the UK and EU provisionally agreed the terms of the UK's withdrawal from the EU. At the time of writing (8 April 2019), it is still very unclear as to when or what the final outcome of EU Exit will be. Leaving the EU will result in several changes that will affect, for example, businesses, individual citizens, the local economy, workforce, regulatory services and communities. However, until the final outcome is known it is difficult to determine its exact impact. Due to the ongoing high degree of uncertainty businesses, organisations and citizens will need to be prepared for all eventualities (including a no deal exit) at national, regional and local levels

Likelihood	Impact	Gross risk without controls
4	4	16

Existing Controls		Responsibility for existing controls
1	The Council's Corporate Risk and Resilience Group is monitoring the potential local impact of EU Exit planning, analysing risk and considering the implications for Gateshead whilst assessing the Council's readiness to respond until a final agreement is known.	Corporate Risk and Resilience Group and all groups and services within the council
2	The Council's Corporate Risk and Resilience Group is identifying any relevant mitigations and controls using existing Business Continuity; Resilience and Emergency Planning; Financial Plans and processes	Corporate Risk and Resilience Group and all groups and services within the council
3	Full engagement and involvement with the Northumbria Local Resilience Forum with Category 1 and 2 multi-agency partner organisations to ensure collaboration with regular reporting by exception to MHCLG	Emergency Planning, Resilience and Response Manager to coordinate
4	A Local Authority information and reporting network has been established led by the Chief Executive from South Tyneside with links into national policy	Emergency Planning, Resilience and Response Manager to coordinate

5	Regular monitoring and reporting by exception on key issues for example, a Cabinet Report was presented on 19 March 2019 of the current position statement	Emergency Planning, Resilience and Response Manager to coordinate

Likelihood	Impact	Net risk after controls
4	3	12

Planned Controls		Responsibility for proposed controls	Target date	Progress
1	Review of the Corporate Continuity Plan and individual service Business Continuity plans to improve response and mitigate the impact of any potential service disruption.	Deputy Strategic Director, Corporate Resources and all Service Directors	April 2019	In progress
2	Future Corporate Resources Overview and Scrutiny Committee review of plans and preparations	Emergency Planning, Resilience and Response Manager	June 2019 onwards	Included on OSC work programme for 2019/2020
3	Identify any lessons learnt following the de-brief process of the approach to planning and preparation	Emergency Planning, Resilience and Response Manager and relevant Service Directors	TBC	TBC

Risk No	Risk Description	Risk Owner
10	**The Council is hit by a Cyber-attack that compromises the confidentiality, integrity and availability of information and systems.**	**Corporate Management Team**

Details of the risk	A successful cyber-attack run against the Council could affect the confidentiality, integrity and availability of all information and systems potentially leading to significant fines and the inability to provide a suitable service to stakeholders.

Likelihood	Impact	Gross risk without controls
4	4	16

Existing Controls		Responsibility for existing controls
1	An approach has been taken to identify baseline technology builds and processes for ensuring the correct configuration management has been implemented. Where possible, unnecessary system functionality is removed or disabled, and known vulnerabilities are mitigated, generally via patching.	Service Directors
2	Appropriate architectural and technical controls have been implemented at all critical access points into the Council's network i.e. to and from the Internet and partner networks. Best practises are followed for all network design and policy implementation.	Service Director – IT Services
3	Users are provided with only the necessary system privileges or data access rights to perform their roles. All elevated permission sets above the norm must be appropriately authorised.	Service Directors
4	Effective policies relating to the appropriate use of IT systems are reviewed annually and issued to all users. All users must confirm that they have read and understood the IT Security Policy before they can log in to the network (A 2-week grace period is generally granted).	Service Directors
5	Best of breed anti-malware technologies are implemented	Service Director – IT Services

	on all endpoints and at relevant gateways as a 'defence in depth' approach.	
6	A protective monitoring solution is in place which aims to help detect actual or attempted attacks on systems and Council Services.	Service Director – IT Services
7	Mobile working and Agile device policies are available for all relevant users. Technical controls are in place using Citrix and Microsoft Intune to reduce the risk of compromise or loss of data.	Service Directors
8	All critical services are appropriately backed up to avoid a significant loss of data.	Service Directors

Likelihood	**Impact**	**Net risk after controls**
3	4	12

Planned Controls		**Responsibility for proposed controls**
1	New User IT Induction to be centred around the Council's IT Security Policy.	Service Directors – IT. Legal and HR
2	Cyber Risks to be built into Operational Risk register	Service Directors
3	Update the existing protective monitoring solution to give greater visibility.	Service Director – IT Services
4	Implement a council wide programme of Cyber Security awareness best practice process, procedures and ways of working including advice on information classification and control.	Service Directors IT Services and Legal