

## Appendix 2 - Q3 2022/23 SUMMARY OF RISK PERFORMANCE

Live or Managed risk	Risk Ref	Risk	Inherent Risk Score	Q3 21/22 Current Risk Score	Q4 21/22 Current Risk Score	Q1 22/23 Current Risk Score	Q2 22/23 Current Risk Score	Q3 22/23 Current Risk Score	Movement	Definition (current score) (L-likelihood) (I-impact)	Owner	Portfolio	Link to Council Plan
L	SR09B	Failure to meet the needs of children and young people	BII	BII	BII	BII	BII	BII	→	L – high I – major	Director of People – Children and Adults Services	Children's Services, and Education & Schools	People
L	SR39	Financial Pressures on SEN Budgets	BII	BII	BII	BII	BII	BII	→	L – high I – major	Assistant Director Education and SEND	Children's Services, and Education & Schools	People
L	SR03B	Finances	AI	AI	AI	AI	AI	AI	→	L – very high I – catastrophic	Chief Finance Officer	Leader	All Values
L	SR46	Medway's Economic Recovery from Covid19	BII	BII	BII	BII	BII	BII	→	L – high I – major	Assistant Director Regeneration	Leader	All Values
L	SR36	Alternative service delivery models	BII	BIII	BIII	BIII	BIII	BIII	→	L – high I – moderate	Assistant Director Regeneration, Chief Operating Officer	Leader	All Values
M	SR37	Cyber Security	AI	AI	AI	CI	CI	CI	→	L – significant I – catastrophic	Chief Information Officer	Resources	All Values
M	SR32	Data and information	BII	CII	CII	CII	CII	CII	→	L – significant I – major	Director of People, Assistant Director Legal & Governance, Chief Information Officer	Resources	All Values
L	SR49	Income Reduction due to Covid19	AI	CII	CII	CII	CII	CII	→	L – significant I – major	Chief Finance Officer	Leader	All Values
M	SR02	Business continuity and emergency planning	CI	DII	DII	DII	DII	DII	→	L – low I – major	Director of Place and Deputy Chief Executive, Chief Organisational Culture Officer	Business Management	All Values

## Q3 2022/23 RISKS

Risk Ref	Risk	Inherent risk (before controls)	Current Controls	Current risk (after controls)	Proposed / Further Controls / Treatment Action	Target risk (after further action)
SR09B	Failure to meet the needs of children and young people	<b>BII</b>	<ul style="list-style-type: none"> <li>SR09.18: Ensure a stable and competent workforce</li> <li>SR09B.19: Delivery of the Improvement Plan</li> <li>SR09B.20: Ensure sufficiency of provision</li> <li></li> </ul>	<b>BII</b>	<ul style="list-style-type: none"> <li>Rethink services and ways of working with families.</li> <li>Managing demand for services.</li> <li>Management of foster care and the residential market.</li> <li>Medium term financial sustainability.</li> <li>Finalise and implement refreshed practice standards.</li> <li>Simplify practice expectations – focus on children’s lived experiences and on promoting quality and consistency of recording to evidence purposeful planning and intervention.</li> <li>Continue our evaluation work in respect of the application of thresholds so that we can be confident that children are supported at the right level.</li> <li>Continue the work already underway to strengthen the effectiveness of our intervention with children in need.</li> <li>Implement our plans to improve our response to neglect, ensure robust implementation of the use of the graded care profile, and evaluate the difference this makes to children’s lives.</li> <li>Continue the work to improve the quality of plans for children in need of protection.</li> <li>Fully implement the strategy in relation to contextual safeguarding for adolescents who are at risk outside the home/family and take time to reflect on themes from Return Home Interviews (RHIs), to create effective safety plans.</li> <li>Support front line managers to oversee and reflect on practice to improve quality of plans and interventions.</li> </ul> <p>Continue to focus on recruitment, retention and career development of our staff.</p>	<b>DIII</b>
SR39	Financial Pressures on SEN Budgets	<b>BII</b>	<ul style="list-style-type: none"> <li>SR39.01: SEN budgets are being closely monitored and spend is being reviewed more robustly.</li> </ul>	<b>BII</b>	<p>A revised high needs deficit recovery plan is in place and will take four years for the council to achieve a positive in-year balance. We will keep pressing the Department for Education (DfE) / Education and Skills Funding Agency (ESFA) for the level of financial support made available to the five Local Authorities (LAs) already awarded emergency High Needs Budget (HNB) recovery funding.</p> <p>Medway was notified in February 2022 that we will be invited to take part in the ‘safety valve’ intervention programme with the DfE in the 2022-23 financial year. The aim of the programme is to agree a package of reform to the high needs system that will bring the dedicated schools grant (DSG) deficit under control. We are currently in conversations with the DfE and ESFA following further details regarding the Safety Valve Intervention Programme (SVIP) and are working to have a High Needs Deficit Recovery Plan by the end of June, to take through the relevant governance route, ahead of the final deadline in September 2022.</p>	<b>DIII</b>
SR03B	Finances	<b>AI</b>	<ul style="list-style-type: none"> <li>SR03B.01: Need to ensure effective response to the spending review, but also lobbying for greater local powers to raise revenues</li> </ul>	<b>AI</b>	The key to improving the effectiveness of the council’s financial planning and management is to address the uncertainty around future funding and improve the forecasting of cost pressures. The failure of central government	<b>CIII</b>

Risk Ref	Risk	Inherent risk (before controls)	Current Controls	Current risk (after controls)	Proposed / Further Controls / Treatment Action	Target risk (after further action)
			<ul style="list-style-type: none"> <li>SR03B.02: Align priorities and activity of the council to resource availability through the MTFs process</li> <li>SR03B.03: Create resources for investment priorities</li> <li>SR03B.04: Delivery of digital transformation programme</li> </ul>		to articulate how it intends to ensure the sustainability of local government has made this task virtually impossible, however the Finance Management team continue to work closely with colleagues within the Planning and Regeneration teams with a view to more accurately projecting future council tax and business rates. The Covid19 pandemic continues to cause far-reaching impacts, not least on the council's financial sustainability, and has exacerbated how challenging it is to project future resources. However, it has also offered an opportunity and impetus to review the types of services we offer and the way we provide them.	
SR46	Medway's Economic Recovery from Covid19	<b>BII</b>	<ul style="list-style-type: none"> <li>SR46.01: Multi-agency Economy Cell and Infrastructure for Recovery established including liaison with the Kent Resilience Forum Economic Recovery Cell</li> <li>SR46.02: Delivery of government-directed financial support to businesses and individuals</li> <li>SR46.03: Reopening High Streets Safely</li> <li>SR46.04: Supporting Medway's businesses</li> <li>SR46.05: Supporting residents' skills and employability</li> <li>SR46.06: Review Medway Council's Strategy base, and resultant regeneration and other programmes to ensure clarity of focus on delivery of economic growth</li> <li>SR46.07: Continue to lobby government to maximise support and opportunities for Medway</li> </ul>	<b>BII</b>	<ul style="list-style-type: none"> <li>Commercial moves out of London – Medway as an attractive place to locate and do business.</li> <li>Rise in working from home / associated decline in commuting means residents spend more leisure and social time and money locally.</li> <li>Innovation Park Medway (IPM) plans reshaped to support the post-Covid19 economy.</li> <li>Opportunity to significantly advance digital inclusion for workers, learners and service users across Medway.</li> </ul>	<b>CII</b>
SR36	Alternative service delivery models	<b>BII</b>	<ul style="list-style-type: none"> <li>SR36.01: Robust options appraisals, and detailed business cases prepared</li> <li>SR36.02: Project management approach to implementation</li> <li>SR36.03: Communication and stakeholder management</li> <li>SR36.04: Sound legal and procurement advice on chosen delivery model</li> <li>SR36.05: Robust scrutiny / oversight mechanisms to ensure clear corporate understanding</li> <li>SR36.06: Reporting from and on delivery models with clear outcomes</li> <li>SR36.07: Business continuity arrangements</li> </ul>	<b>BIII</b>	<p>The decision taken by the council in February 2022 to bring back the recruitment agency from Kyndi, whilst representing a challenge for the company, also offers an opportunity to rethink its strategy and focus on growing the telecare and CCTV services.</p> <ul style="list-style-type: none"> <li>Medway Development Company (MDC) Ltd. has established a subsidiary and is now considering the business case for entering the private rented sector, as a strategy for ensuring its longer-term future.</li> </ul>	<b>CIII</b>
SR37	Cyber Security	<b>AI</b>	<ul style="list-style-type: none"> <li>SR37.01: Secure configuration: Remove or disable unnecessary functionality from systems, and to quickly fix known vulnerabilities</li> <li>SR37.02: Network security: Create and implement policies and appropriate architectural and technical responses, thereby reducing the chances of attacks succeeding</li> <li>SR37.03: Managing user privileges: All users should be provided with a reasonable (but minimal) level of system privileges and rights needed for their role. The granting of highly elevated system privileges should be carefully controlled and managed.</li> </ul>	<b>CI</b>	<p>Work commenced in preparing for the pre-requisites to obtain Cyber Essential Plus accreditation. Due to Covid19 this work has been paused as it is not an essential requirement to obtain this accreditation, however the work in improving cyber security has continued. The results from our PSN scan will be included in our Cyber Essentials application in October 2022.</p> <p>The ICT Network &amp; Cyber Security Manager has specific responsibilities for the security of the network, overseeing user privileges and security policies, and user education and awareness.</p> <p>System monitoring software tools are being reviewed to determine whether there are solutions that will further strengthen the cyber security measures already in place.</p>	<b>CI</b>

Risk Ref	Risk	Inherent risk (before controls)	Current Controls	Current risk (after controls)	Proposed / Further Controls / Treatment Action	Target risk (after further action)
			<ul style="list-style-type: none"> <li>• SR37.04: User education and awareness: Users have a critical role to play in their organisation's security and so it's important that security rules and the technology provided enable users to do their job as well as help keep the organisation secure. This can be supported by a systematic delivery of awareness programmes and training that deliver security expertise as well as helping to establish a security-conscious culture</li> <li>• SR37.05: Incident management: All organisations will experience security incidents at some point. Investment in establishing effective incident management policies and processes will help to improve resilience, support business continuity, improve customer and stakeholder confidence and potentially reduce any impact.</li> <li>• SR37.06: Malware prevention: Malicious software, or malware, is an umbrella term to cover any code or content that could have a malicious, undesirable impact on systems. Any exchange of information carries with it a degree of risk that malware might be exchanged, which could seriously impact your systems and services. The risk may be reduced by developing and implementing appropriate anti-malware policies as part of an overall 'defence in depth' approach.</li> <li>• SR37.07: Monitoring: System monitoring provides a capability that aims to detect actual or attempted attacks on systems and business services. Good monitoring is essential in order to effectively respond to attacks. In addition, monitoring allows you to ensure that systems are being used appropriately in accordance with organisational policies. Monitoring is often a key capability needed to comply with legal or regulatory requirements</li> <li>• SR37.08: Removable media controls: Removable media provide a common route for the introduction of malware and the accidental or deliberate export of sensitive data. You should be clear about the business need to use removable media and apply appropriate security controls to its use.</li> <li>• SR37.09: Home and mobile working: Mobile working and remote system access offers great benefits but exposes new risks that need to be managed. You should establish risk-based policies and procedures that support mobile working or remote access to systems that are applicable to users, as well as service providers. Train users on the secure use of their mobile devices in the environments they are likely to be working in.</li> </ul>		<p>Endpoint device protection (protecting the end user devices) – areas have been found for improvement to ensure that should an individual's machine be infected with ransomware, the ransomware could potentially manoeuvre laterally within that network segment. Reviews of solutions to address this issue have taken place and some indicative costs have been received. This is to be reflected on ICT's Medium Term Financial Strategy (MTFS) strategy to address how the solution could be funded.</p> <p>Immutable backups – There have been several councils hit by ransomware recently and one of the key lessons learned from those events is that the recovery process could have been drastically improved if the councils had immutable copies of the backup data. What this means is that the disks and the data are not able to be encrypted by a ransomware attack.</p> <p>ICT have been reviewing guidance provided by the National Cyber Security Centre (NCSC). We are actively reviewing systems and applications to ensure they are up to the latest version. An area that needs to be addressed is the formation of a formal Cyber Security Incident Response team (CSIRT). The core team will usually be ICT and Cyber Security staff. The extended team may include other capabilities such as the Communications, Human Resources (HR) and Legal teams. Training for key contributors is currently being identified.</p> <p>The ICT team is monitoring the situation closely and keeping a watchful eye on suspicious traffic. There has been an increase in phishing email attempts however these have not shown to have originated from Russia or are related to this situation at present.</p>	

Risk Ref	Risk	Inherent risk (before controls)	Current Controls	Current risk (after controls)	Proposed / Further Controls / Treatment Action	Target risk (after further action)
			<ul style="list-style-type: none"> <li>SR37.10. Robust policies and procedures in place: Robust policies and procedures in place that are audited internally and externally. The council is accredited against the Public Service Network (PSN) code of connection criteria that provides assurances that the ICT infrastructure is managed and monitored using methods commensurate with recognised good practice and the guidance issued by CESG (the UK government's National Technical Authority for Information Assurance). Following the advice and guidance issued by the National Cyber Security Centre (NSCS) to help organisations bolster their cyber defence.</li> </ul>			
SR32	Data and information Management	<b>BII</b>	<ul style="list-style-type: none"> <li>SR32.01: The council has accountability and governance in place for data protection and data security</li> <li>SR32.05: Staff are supported in understanding their obligations under the National Data Guardian's Data Security Standards</li> <li>SR32.06: Appropriate policies and procedures are in place to support good information management and security</li> </ul>	<b>CII</b>	Review support for information governance within the organisation. Audit the council's Data Security and Protection (DSP) Toolkit submission internally to ensure continual improvement. Appoint a deputy SIRO. Seeking Public Services Network (PSN) Compliance	<b>DIII</b>
SR49	Income Reduction due to Covid19	<b>AI</b>	<ul style="list-style-type: none"> <li>SR49.01: Priority is being given to structuring our operations to provide customers with confidence about returning to Covid19 compliant facilities and events. The focus is on restoring income levels in 2022/23, as the council and local economy recovers from the effects of the pandemic. This will require ongoing support from the Communications and Marketing team.</li> <li>SR49.04: In the next financial year, a smart parking pilot will be implemented.</li> <li>SR49.05: Enhanced promotion of our Front-Line trading services e.g. weddings, green space sports (tennis, pitch and put, football pitches)</li> <li>SR49.06: Adults' Social Care</li> </ul>	<b>CII</b>	Income has largely returned to pre-Covid19 levels, although there is now a 'hangover' in terms of debt collection, particularly in terms of rental income. Officers are working with tenants and other debtors to recover income due.	<b>CII</b>
SR02	Business continuity and emergency planning	<b>CI</b>	<ul style="list-style-type: none"> <li>SR02.01: Continued review and develop the Council's Major Emergency Plan (MEP) including any Lessons Identified</li> <li>SR02.02: Business continuity plans completed to implement the actions</li> </ul>	<b>DII</b>	<u>Emergency Planning</u> The Covid19 emergency allowed for a faster solution to the remote working problem. If properly applied, problems like snow and fuel disruption will be eased slightly because of this project. <u>Business Continuity</u> As a result of Covid19, the Corporate Business Continuity Plan and Business Continuity (BC) training will be reviewed to include best practice, lessons learnt, and observations made from the council's response and recovery plans. Cabinet received a paper on the council's Covid19 response on 7 July 2020 and Covid19 recovery on 25 August 2020.	<b>DII</b>

Risk Ref	Risk	Inherent risk (before controls)	Current Controls	Current risk (after controls)	Proposed / Further Controls / Treatment Action	Target risk (after further action)
					<p>Council services refreshed their business continuity plans in October 2020 in preparation for the Covid19 pandemic second wave and European Union (EU) exit by 31 December 2021.</p> <p>Business Support Overview and Scrutiny committee received a paper on 28 January 2021 on the risk environment to consider the wider risk environment facing the council, including the differences between the Corporate Risk Register, business continuity and emergency planning.</p> <p>Cabinet and Business Support Overview and Scrutiny committee received a paper on 30 March 2021 on the council's Covid19 Response and Recovery actions and plans.</p>	