



Information Governance Risk Register

Likelihood	4 Almost Certain				
	3 Probable				
	2 Possible				
	1 Hardly Ever				
		1 Negligible	2 Minor	3 Major	4 Critical
	Impact				

REVIEWED DATES:

Tool 1. Risk Appetites – Hungry, Opportunist, Creative and Aware, Cautious, Averse

Those “green” risks that have been on the risk register for 6 months or more can now be classed as “business as usual” risk and therefore be removed from the register

The matrix below, helps you define where the risk is by scoring it on a basis

4 Almost certain	Retain	Transfer Modify Retain	Avoid Transfer Modify	Avoid Transfer Modify
3 Probable	Retain	Prioritise for Modifying Retain	Transfer Modify Retain	Avoid Transfer Modify
2 Possible	Retain	Prioritise for Modifying Retain	Prioritise for Modifying Retain	Transfer Modify Retain
1 Hardly ever	Retain	Retain	Retain	Prioritise for Modifying Retain

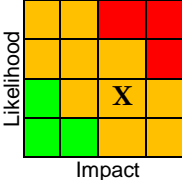
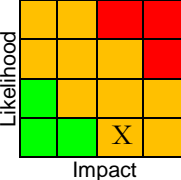
Description of occurrence

- Occurs several times per year. It will happen.
- It has happened before and could happen again.
- It may happen but it would be unusual.
- Never heard of it occurring. We can't imagine it occurring.

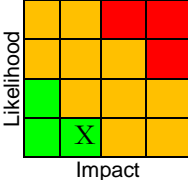
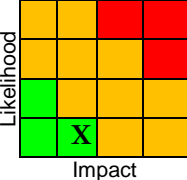
Impact	Service Delivery	Finance	Reputation	People
Critical (4)	Prolonged interruption to service	Severe costs incurred	Adverse national coverage with significant change in stakeholder confidence	Fatality, disability or serious long term health problem
Major (3)	Key targets missed- some service compromised	Significant costs incurred	Adverse local media coverage with moderate change in stakeholder confidence	Series injuries. Exposure to dangerous conditions
Minor (2)	Management action required to over short – term difficulties	Some costs incurred (handled within management budgets)	Adverse local media for 1-7 days	Minor injuries or discomfort. Feeling unease
Negligible (1)	Handled within day to day routines	Little loss anticipated	No significant comment or media coverage	No injury

1 Negligible	2 Minor	3 Major	4 Critical
-------------------------	--------------------	--------------------	-----------------------

Appendix A- Information Governance Risk Register September 2021

Risk No:	Risk Description (Failure to/Lack of...)	Risk Owner	Risk Appetite (How much risk are we prepared to take and the total impact of the risk we are prepared to accept)	Current Controls/Actions	Current Risk Score	Target Risk Score at end of	Assurance - Status (Full, Substantial, Limited, No)	Assurance - Direction of Travel (Improving, Static, Declining)
1.	<p>Data protection training</p> <p>Risk – Information is inappropriately shared, lost or handled due to lack of training or failure to complete, renew or follow up non completion– leading to non-compliance, enforcement action, compensation claims, reputational damage and monetary fines.</p> <p>Legislation- Article 5(f) of UK GDPR security and Article 32-testing effectiveness of security.</p>	DPO/B DITM	Averse	<p>Controls in place: e-learning currently on intranet and low risk training form. New starters required to complete training on induction. Members and IAOs receive training. SIRO external training Sep 19.</p> <p>Further action required/anticipated completion date: Renewal of training annual.</p> <p>Responsibility: IAO's, DPO, BDITM, CLT.</p> <p>Milestones: Renewal of training for 2021 due and new e-learning with cyber security to be rolled out and completed by December 2021.</p> <p>Low risk forms to be rolled out again. IAO responsibility to ensure completion of training. Staff to update own training records on I Trent. Non-completion to be followed up (IAO's and DPO)</p> <p>March 2021 all staff on network accepted Data Protection and SAR summary sheet (included updated to DP Policy and SAR responsibilities.</p> <p>Target date (s): Annually and non-completion followed up. 2019-89% 2020-86% 2021- 84% DP and SAR sheet (completion higher as remaining 17% now locked out the network so non-completers likely to be staff recently left, those who complete low risk form and don't use the network) Work planned with IT to resolve.</p>			Substantial	Declining

Appendix A- Information Governance Risk Register September 2021

Risk No:	Risk Description (Failure to/Lack of...)	Risk Owner	Risk Appetite (How much risk are we prepared to take and the total impact of the risk we are prepared to accept)	Current Controls/Actions	Current Risk Score	Target Risk Score at end of	Assurance - Status (Full, Substantial, Limited, No)	Assurance - Direction of Travel (Improving, Static, Declining)
2.	<p>Comms</p> <p>Risk - Information is inappropriately shared, lost or handled due to a lack of awareness of data protection due to absence of or ineffective communications – leading to non-compliance, enforcement action, compensation claims, reputational damage and monetary fines.</p> <p>Legislation - Article 32 UK GDPR security</p>	COMM S/DPO	Cautious	<p>Controls in place: Current comms plan in place, comms attend IG working group- quarterly basis. Posters on stairwells, articles on intranet. Regular posts on data protectors’ forum by IG team.</p> <p>Further action required/anticipated completion date: To continue with plan, issue regular comms on fines, email use and breaches. DPO issuing regular posts on data protectors. DP standing item at SMTF-monthly. Comms issued on home working during pandemic, protecting council data working remotely, Teams and O365 including guidance on recording Teams meetings. Comms on Brexit and UK GDPR Comms on 3 yrs of GDPR day</p> <p>Overall Responsibility: DPO, Comms, CLT</p> <p>Milestones: Comms plan (COMMS/DPO) Reactive comms (COMMS/DPO)</p> <p>Target date (s): Delivery of ongoing Comms plan and reactive Comms.</p>			Substantial	Static

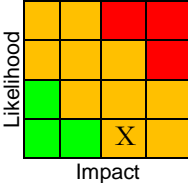
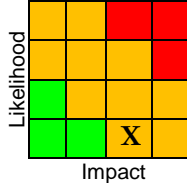
Appendix A- Information Governance Risk Register September 2021

Risk No:	Risk Description (Failure to/Lack of...)	Risk Owner	Risk Appetite (How much risk are we prepared to take and the total impact of the risk we are prepared to accept)	Current Controls/Actions	Current Risk Score	Target Risk Score at end of	Assurance - Status (Full, Substantial, Limited, No)	Assurance - Direction of Travel (Improving, Static, Declining)
3.	<p>Policies and procedures</p> <p>Risk – Information is inappropriately shared, lost or handled due to a lack of policies or policies becoming out of date/ inaccurate/not communicated/not in place, not approved – leading to non-compliance, enforcement action, compensation claims, reputational damage and monetary fines.</p> <p>Legislation - Article 5(f)-security and Article 32-testing- UK GDPR</p>	IAO's/ DPO	Averse	<p>Controls in place: IM polices were updated in 2018. The updates to the Data Protection Policy and SAR Summary sheet were accepted by all staff on net-consent in March 2021.</p> <p>Further action required/anticipated completion date: Policies to be reviewed as and when required and every 2 years.</p> <p>Overall Responsibility: DPO, CLT.</p> <p>Milestones: Special category policy (DPO) now drafted and published. IM policies review for 2021 complete.</p> <p>Target date: Policies to be reviewed as and when required and every 2 years.</p>			Substantial	Static
4.	<p>Information Asset Register and Records of Processing (ROPA)</p> <p>Risk- Lack of a ROPA or failure to keep up to date resulting in data not being treated correctly leading to non-compliance, enforcement action, compensation claims, reputational damage and monetary fines.</p> <p>Legislation- Article 30 UK GDPR- ROPA</p>	IAO's/ DPO	Averse	<p>Controls in place: CoLC has an IAR which forms the ROPA. IAO's have been provided with their section of the register. IAO's confirm in an annual checklist to have risk assessed their information assets and when required.</p> <p>Further action required/anticipated completion date: The IAR needs to be kept up to date and risk assessed regularly by IAO's. Has been placed in services managers area and regular updates to IAO's to check and update at SMTF</p> <p>Overall Responsibility: IAO's, DPO, CLT.</p> <p>Milestones: IAO Handbook updated Jan</p>			Substantial	Static

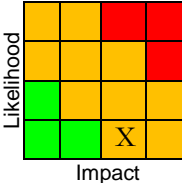
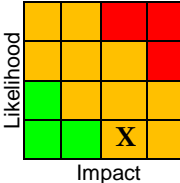
Appendix A- Information Governance Risk Register September 2021

Risk No:	Risk Description (Failure to/Lack of...)	Risk Owner	Risk Appetite (How much risk are we prepared to take and the total impact of the risk we are prepared to accept)	Current Controls/Actions	Current Risk Score	Target Risk Score at end of	Assurance - Status (Full, Substantial, Limited, No)	Assurance - Direction of Travel (Improving, Static, Declining)
				2021 and uploaded to net-consent. Annual IAO Checklist last issued Nov 19. Delayed due to response to pandemic. IAO Training to be delivered in 2021 and checklists reissued (DPO) IAR placed on service managers drive. IAO handover included in HR checklist. Target date: IAO's to review and update and complete Checklist for 2021. Planned for Autumn 2021. Reminders to review ROPA provided to all IAO's and an Action for all IAO's at each SMTF in 2021 to date. Mini audits on checklist and compliance (DPO, Audit,) including risks from pandemic data collection and sharing to be added to IAO Checklist.				
5.	<p>Retention and disposal of personal data/records.</p> <p>Risk- Personal data is kept longer than necessary leading to increase in volume of data compromised in a data breach and/or over complicating Data Subject Requests- leading to non-compliance, enforcement action, compensation claims, reputational damage and monetary fines.</p> <p>Legislation- Article 5(e) UK GDPR storage limitation.</p>	IAO's/ DPO/B DITM	Averse	<p>Controls in place: Retention schedules were updated in 2018 and available to staff on intranet and on website. IAO's confirm in an annual checklist that retention and disposal is being implemented.</p> <p>Further action required/anticipated completion date: Retention in systems and electronic storage remains to be an issue and needs to be automated as far as possible.</p> <p>Overall Responsibility: DPO, BDITM, IAO's, CLT</p> <p>Milestones: Develop RM action plan with alongside IT</p>			Limited	Static

Appendix A- Information Governance Risk Register September 2021

Risk No:	Risk Description (Failure to/Lack of...)	Risk Owner	Risk Appetite (How much risk are we prepared to take and the total impact of the risk we are prepared to accept)	Current Controls/Actions	Current Risk Score	Target Risk Score at end of	Assurance - Status (Full, Substantial, Limited, No)	Assurance - Direction of Travel (Improving, Static, Declining)
				Strategy and Office 365/Microsoft Teams. (BDIT) Mini audits on service areas and systems (DPO, Audit,) BDIT-carrying out work on deleting data from Authority Wide Target date (s) Tackle with changes to IT Infrastructure. Work is currently being undertaken on retention and sensitivity labelling in Office 365 and report is to be submitted to CMT on options available. DPIA drafted for O365 and shared with consultants who approved. Includes need for retention and consideration of IG tools. O365 to be rolled out to all by September 2021.				
6.	Information Sharing Agreements (ISA's) (sharing with partners) Risk- Information is inappropriately shared, lost or handled by CLC or partner due to lack of an ISA or an appropriate ISA or due to an out of date ISA. Legislation- Article 26 UK GDPR (joint controllers) and Article 5(f)-security	IAO's/ DPO	Averse	Controls in place: ISA template updated for GDPR 2018. List of ISA's in progress. ISA's being implemented and reviewed. Further action required/anticipated completion date: Need to continue to identify areas requiring ISA's. Need to ensure ISA's are reviewed. Overall Responsibility: DPO, IAO's, CLT Milestones: ISA list to published for IAO's to review Covered at IAO training. Reminders issued at SMTF regularly. Template has been reviewed for 2021 and changes in GDPR.			Substantial	Static

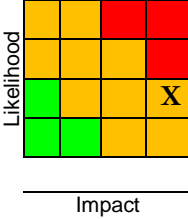
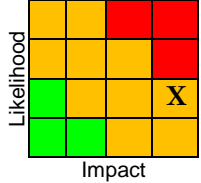
Appendix A- Information Governance Risk Register September 2021

Risk No:	Risk Description (Failure to/Lack of...)	Risk Owner	Risk Appetite (How much risk are we prepared to take and the total impact of the risk we are prepared to accept)	Current Controls/Actions	Current Risk Score	Target Risk Score at end of	Assurance - Status (Full, Substantial, Limited, No)	Assurance - Direction of Travel (Improving, Static, Declining)
				<p>Target date (s) ISA list was published on service manager's drive and asset owners' responsibilities to update and ensure agreements are reviewed. Reminders to review ISA list provided to all IAO's and an Action for all IAO's at each SMTF in 2021 to date. Target to share with other LA's in county and compare.</p>				
7.	<p>Information sharing- with data processors (contracts with suppliers).</p> <p>Risk – information is inappropriately shared, lost or handled incorrectly by processors or sub processors due to contracts not being in place, not containing UK GDPR clauses, not in correct form, not approved/signed-leading to non-compliance, enforcement action, compensation claims, reputational damage and monetary fines.</p> <p>Legislation- Article 28-Processors UK GDPR</p>	IAO's/ DPO/L DSM/P rocurement	Averse	<p>Controls in place: A comprehensive list of contracts has been compiled and uploaded to the Pro Contract system. Major contracts have now been covered off with GDPR clauses and all new contracts contain the clauses.</p> <p>Further action required/anticipated completion date: Contracts were prioritised according to sensitivity and suppliers contacted to amend contracts. Majority covered off although will be areas where a contract should be in place and contracts not aware of.</p> <p>Overall Responsibility IAO's, Legal Services, DPO, CLT.</p> <p>Milestones: Contracts reviewed on risk based approach according to sensitivity. All new and renewed contracts have clauses.</p> <p>Target date (s) contracts being reviewed on a case-by-case basis.</p> <p>Brexit implications- UK has now</p>			Substantial	Static

Appendix A- Information Governance Risk Register September 2021

Risk No:	Risk Description (Failure to/Lack of...)	Risk Owner	Risk Appetite (How much risk are we prepared to take and the total impact of the risk we are prepared to accept)	Current Controls/Actions	Current Risk Score	Target Risk Score at end of	Assurance - Status (Full, Substantial, Limited, No)	Assurance - Direction of Travel (Improving, Static, Declining)
				received adequacy decision from EU for transfers of data into the UK from EU. Continue to monitor as UK law could change.				
8.	<p>Data subject's rights</p> <p>Risk- failure to respond to a rights request or to respond within statutory time limits resulting from lack of resources, increasing complexity of requests, inadequate privacy notices, deletion being manual in some cases and resource intensive leading to non-compliance, enforcement action, compensation claims, reputational damage and monetary fines</p> <p>Legislation- Articles 12-23 Rights of the data subject</p>	IAO's/ DPO	Averse	<p>Controls in place: Data subject request form and procedure changed to meet new rights. GDPR and Data Protection Policy and Summary sheet setting out rights to staff. Customers informed of rights in privacy notice.</p> <p>Further action required/anticipated completion date: Some systems can only comply with the right to be deleted manually. There may be areas where specific privacy notices have not been provided. Resources need to continue to be monitored as requests increase and become more complicated.</p> <p>Overall Responsibility: IAO's, BDITM, DPO, CLT.</p> <p>Milestones: IAO Checklist IAO training 2021 DPA request type, volume and response rates monitored and reported to CLT quarterly. 2021-SAR application on website to be made into an e-form to improve accessibility. Improved tools to automate SAR's in O365 environment training being considered although current policies do not support automated email searches of officers accounts unless request.</p>			Substantial	Static

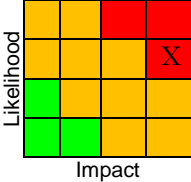
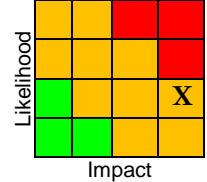
Appendix A- Information Governance Risk Register September 2021

Risk No:	Risk Description (Failure to/Lack of...)	Risk Owner	Risk Appetite (How much risk are we prepared to take and the total impact of the risk we are prepared to accept)	Current Controls/Actions	Current Risk Score	Target Risk Score at end of	Assurance - Status (Full, Substantial, Limited, No)	Assurance - Direction of Travel (Improving, Static, Declining)
9.	<p>Data breaches</p> <p>Risk- breaches are not identified or responded to accordance with the data breach management policy due to lack of awareness of a data breach of policy/procedures, staff not wanting to report breaches, not analysing the causes of breaches to prevent reoccurrence, not reporting required breaches to the ICO-leading to non-compliance, enforcement action, compensation claims, reputational damage and monetary fines.</p> <p>Legislation-Articles 33 and 34 UK GDPR Notification and communication of a personal data breach.</p>	IAO's/ DPO	Averse	<p>Controls in place: Data breach management policy implemented. Internal e-form reporting procedure for staff. Data breach register kept and analysed for trends and where relevant mitigation put in place. Breaches reported to ICO and data subjects where required. Breaches including type, volume, service area and action taken reported to CLT on bi annual basis.</p> <p>Further action required/anticipated completion date: Always an ongoing risk despite procedures that a breach may occur. Ongoing monitoring and management required.</p> <p>Overall Responsibility: IAO's, DPO, CLT</p> <p>Milestones: Ongoing comms/awareness/training/ Compliance checks. Internal Audit spot checked breaches for compliance with our management policy in June 19. Good practice by CoLC was recognised in this area. No significant increase in breaches during increased home working due to pandemic.</p>			Substantial	Static

Appendix A- Information Governance Risk Register September 2021

Risk No:	Risk Description (Failure to/Lack of...)	Risk Owner	Risk Appetite (How much risk are we prepared to take and the total impact of the risk we are prepared to accept)	Current Controls/Actions	Current Risk Score	Target Risk Score at end of	Assurance - Status (Full, Substantial, Limited, No)	Assurance - Direction of Travel (Improving, Static, Declining)
10.	<p>Data Protection Impact Assessments (DPIA)</p> <p>Risk – information is inappropriately shared, lost or handled incorrectly due to privacy risks not being addressed in a DPIA for high risk processing of personal data, due to lack of awareness when to carry out, lack of willingness to carry out or allocate time and resources to complete or assessments being inadequate-leading to non-compliance, enforcement action, compensation claims, reputational damage and monetary fines.</p> <p>Legislation- Article 35-DPIA</p>	IAO's/ DPO	Averse	<p>Controls in place: A DPIA process has been put in place with guidance for staff on City people. The DPIA process has imbedded in the Lincoln Project Management Model. DPIA are covered in policies and IAO Handbook and training and in annual IAO Checklist.</p> <p>Further action required/anticipated completion date: Take up of DPIA's has been low. The template may need amending to be more user friendly and relaunched again with Comms and training.</p> <p>Overall Responsibility: IAO's, DPO BDIT, CLT.</p> <p>Milestones: Revise template and guidance Comms/awareness/training/compliance checks Part of LMMP process</p> <p>Target dates: New DPIA template has been drafted and is being trialled. Number of DPIA's during pandemic due to increased sharing.</p>			Substantial	Static

Appendix A- Information Governance Risk Register September 2021

Risk No:	Risk Description (Failure to/Lack of...)	Risk Owner	Risk Appetite (How much risk are we prepared to take and the total impact of the risk we are prepared to accept)	Current Controls/Actions	Current Risk Score	Target Risk Score at end of	Assurance - Status (Full, Substantial, Limited, No)	Assurance - Direction of Travel (Improving, Static, Declining)
11	<p>Security of personal data- including physical and IT security.</p> <p>Risk- – information is inappropriately shared, lost or handled incorrectly due to failure of or lack of IT security and physical security of data- leading to data breaches, cyber-attacks, loss of data, inappropriate access, retention of old data and non-compliance leading to enforcement action, fines, adverse publicity/reputational damage, compensation claims and impact on business continuity.</p> <p>Legislation- Article 5 and 32-Security (integrity and confidentiality) and testing of security measures.</p>	IAO's/ DPO/B DITM	Averse	<p>Controls in place: Clear desk policy, data protection training and IM policies, IT security, access restricted and reviewed by IAO's dependant on job role. Data breach management policy, IT security policies, anti-virus/malware, encryption, TLS secure approved email, access controls.</p> <p>Further action required/anticipated completion date: Security measures to be constantly reviewed and upgraded. Procurement of IT products needs to include due diligence in regard to the security of personal data. IT Security policies need to be updated and reviewed.</p> <p>Overall Responsibility: BDITM, IAO's, CLT, DPO</p> <p>Milestones: Comms/awareness/training Compliance checks and testing</p> <p>Target date(s) -The LGA Cyber Security stock take - action plan will be finalized (key actions), communicated and agreed with AD group (IT Steering group). -Update and approve a new ICT Strategy -The core IT infrastructure will be upgraded/updated -Assist IAO to review access to network drives. -Increased oversight of IT project / programmes by the IT Steering group (AD</p>			Substantial	Declining

Appendix A- Information Governance Risk Register September 2021

Risk No:	Risk Description (Failure to/Lack of...)	Risk Owner	Risk Appetite (How much risk are we prepared to take and the total impact of the risk we are prepared to accept)	Current Controls/Actions	Current Risk Score	Target Risk Score at end of	Assurance - Status (Full, Substantial, Limited, No)	Assurance - Direction of Travel (Improving, Static, Declining)
				group). -Develop/Implement new policy framework -Review ICT DR plan New actions A Cyber/IT risk register has been created. First draft has been considered by CLT has been adapted since in consultation with the council's contracted IT Security Auditor. The register is be finalised by BDITM. IT security policies are currently being updated. Need remote working policy. Need to be prioritised for localising and for approval by policy scrutiny. Upgraded to Red risk in June 2021 due to policy review required, not been a priority due to pandemic and O365 roll out.				

If you were **'hungry'** for risk, you would go straight to the biggest roller coaster in the park, get on the ride, have your hands up in the air and not worry about the risk of the ride breaking down or having a failure somewhere. You would embrace the experience and do it time and time again.

If you were **'opportunist'** you would go to the ride and realise that the wait for the ride was an hour, but you would wait because you would not want to miss this opportunity.

If you were **'creative & aware'** you would probably go on the ride but be a bit more reserved. You would maybe go on a few more smaller rides beforehand and then when it comes to the roller coaster, you would probably be apprehensive, check the seat belts, check other people's reaction coming off the ride and have a general awareness of what the ride operator is doing at every point during the ride. You might enjoy the experience and even have another go.

If you were **'cautious'**, you would go around the park several times during the day, looking up at the roller coaster but you would probably be anxious, scared and would have to be dared to go on the ride. You might consider going on the ride but you would wait until it was nearly time to go home and then be shaking with fear as you walk up and get on the ride. You probably wouldn't go on the ride again but at least you could say you did it, even if it made you feel ill.

If you were **'averse'**, you wouldn't even consider going anywhere near the ride, let alone actually having a go on it.