

Appendix 5

CR 25 GDPR Project Phase 2

Risk no, Title, Creation date, Owner		Current Risk Rating & Score		Risk Update and date of update	Target Risk Rating & Score		Target Date	Current Risk score change indicator
CR25 General Data Protection Regulation Project phase 2	<p>Cause: Inadequate departmental systems and procedures are in place which meet the additional requirements of GDPR legislation.</p> <p>Event: CoL is unable to comply with GDPR requirements - poor, non-secure and non-compliant processing of personal data.</p> <p>Effect: CoL exposed to adverse publicity, reputational damage, financial penalties imposed by the Information Commissioners Office. Increased volume of Subject Access Requests.</p>	<p>Likelihood</p> <p>Impact</p>	6	<p>Progress on high risk areas identified in the Mazars audit:</p> <ul style="list-style-type: none"> • Significant progress has been made toward facilitating departmental compliance with GDPR requirements - see actions. • Significant progress has been made toward ensuring contractor compliance with GDPR requirements - see actions. • An overarching CoLC retention schedule is in place and 75% of departments have responded with detailed retention schedules. • The management of unstructured data constitutes a significant GDPR compliance risk. Four potential suppliers have been identified - see actions 	<p>Likelihood</p> <p>Impact</p>	4	31-Dec-2018	<div style="width: 20px; height: 10px; background-color: blue;"></div>
01-Dec-2017 Michael Cogher				03 Oct 2018				Constant

Appendix 5

CR 25 GDPR Project Phase 2

Action no, Title,			Action owner	Latest Note Date	Due Date
CR25g GDPR Project Phase 2 governance	<ol style="list-style-type: none"> 1. Report to Summit Group 2. report to Audit & Risk Committee 3. Report to IT sub-committee 4. GDPR Project Team meetings 	<ul style="list-style-type: none"> • Project meetings held bi-weekly are effectively monitoring project outputs • Report to Summit October 2018 • Report to Audit & Risk Committee scheduled for 15.11.18 • Report to IT sub-committee 02.11.18 	Michael Cogher	03-Oct-2018	31-Dec-2018
CR25h Departmental Records Retention Schedules	<ul style="list-style-type: none"> • Departments to supply existing records retention schedules to supplement the CoLC corporate retention schedule. • GDPR compliance team to advise and review departmental retention schedules. 	Departmental record retention schedules included in departmental compliance monitor. 64% of departments have responded with details of their retention schedules	Michael Cogher	03-Oct-2018	31-Oct-2018
CR25i Departmental Compliance Audits	<ul style="list-style-type: none"> • Investigation of use of meta compliance tool • If 1 unsuccessful create audit template for departments to complete • GDPR compliance Team review returns and advise departments on non-compliance issues 	<ul style="list-style-type: none"> • Departmental compliance audits issued to depts in September. • Meetings with departmental AIN reps ongoing. • Departmental responses to compliance audits being analysed. 	Michael Cogher; Nick Senior	03-Oct-2018	30-Nov-2018
CR25j Data Privacy Impact Assessment	<ul style="list-style-type: none"> • Refine existing draft DPIA template • Road test • Incorporate into CoLC projects and procurement processes 	Data privacy impact assessments now mainstreamed into CoLC project management methodology and in toolkit on intranet.	Michael Cogher	03-Oct-2018	30-Sep-2018
CR25k GDPR Contractor Compliance	<ul style="list-style-type: none"> • Standard contract clauses developed and applied to all new contracts • Template for departmental use to record and monitor compliance • Will be tested by GDPR compliance Team as part of departmental GDPR audits 	A number of departments have responded supplying details of contractor compliance. Assessment of departmental compliance included in compliance monitor - departments will be chased by DPO in this issue.	Michael Cogher; Nick Senior	03-Oct-2018	31-Dec-2018
CR25l Management of unstructured personal data	<ul style="list-style-type: none"> • Paper to summit group on deletion of W drive data. • Data discovery tool procurement 	Software to identify unstructured personal data is being scoped. Potential suppliers are now set up on Capital esourcing and we await their costs to provide a software data discovery tool to identify where data might be stored at risk (i.e. freely accessible) across the entire CoLC IT estate.	Matt Gosden	03-Oct-2018	31-Dec-2018