Committee(s)	Dated:
Digital Services Sub Committee – For Information	30th May 2019
Subject: IT Division Risk Update	**Public**
Report of: The Chamberlain	**For Information**
Report author: Samantha Kay – IT Business Manager	

Summary

All IT Risks are now in the Risk Management System, with actions included, for the ongoing improvement and continuing assessment to the Management of Risk within the IT Division. The IT Division currently holds 5 risks, a reduction of four from the previous period. There are currently no RED risks. There are no extreme impact risks, there are 4 major impact, 1 serious impact and no Minor impact risks.

IT currently holds 2 risks on the Corporate Risk Register, whilst feeding in to the GDPR Corporate risk which is owned by Comptrollers.

Summary of the Corporate Risks

CR 16 – Information Security - Will continue to be monitored at Corporate level and reviewed for decision at DSSC and Audit & Risk Management Committee in July.

CR 25 – GDPR Regulation Compliance – Will continue to be monitored following the closure of the formal project. It is expected that this will be de-escalated from the Corporate Risk register on the assumption that the internal audit review does not flag any issues of serious concern.

CR 29 – Information Management – Approved by Audit & Risk Committee to be managed as a Corporate Risk.

Recommendation(s)

Members are asked to:
- Note the report.

Main Report

Background

1. Risk remains a key focus for the IT Division and we are continuing to ensure that it drives the priority for project works and Change Management decisions. Regular reviews will ensure the ongoing successful management of these risks across the division

Current Position

2. The IT Division Currently holds 2 Amber risks on the Corporate Risk Register and assists to mitigate one other Amber Corporate Risk. The IT Division currently holds 5 risks, none of which are scored as Red. All risks have owners, clear actions, with target dates to enable focussed management, tracking and regular and consistent reviews.

Current status

3. Since the last report the IT Risk Register has seen the following activity:

   - 2 Risk has been upgraded to Corporate level.
   - 2 Risks have been reduced from Departmental to Divisional level.
   - 1 Risk has been deactivated
   - 3 Risks reduced in score

   The remainder are static and continue to be monitored alongside the relevant on-going projects.

Movement of Risks

4. **Movement from Departmental to Corporate**
   - **CR16 Information Security** – Will continue to be monitored at Corporate level, with a review at DSSC and A&RMC in July.
   - **CR29 Information Management** – Approved by Audit & Risk Committee to be managed as a Corporate Risk. The focus will be to deliver the IM Strategy through a series of actions that are documented in the risk system. (See Appendix A for the details of this risk).

5. **Risks reduced from Departmental to Divisional Level**

   The following risks have been reduced to division level due to mitigating actions being completed, and processes implemented to maintain systems going forward.

   - **CHB IT 001 Resilience - Power and infrastructure**–An ongoing project has started to audit all requirements and make recommendations.
   - **CHB IT 014 Software Lifecycle Mgt –** Following improvements in processes, application rationalisation & more detailed service reviews.

6. **Risks that have been deactivated**

- **CHB IT 028 IP Telephony and Call recording - Funding Requirements** – Funding for project has been provisioned thus mitigating this risk.

7. **Risks that have reduced in score**

- **CHB IT 026 Failure to commence CoLP IT Modernisation** – Funding has been provisioned for the project thus lowering the likelihood. The risk will now be revaluated with respect to the delivery of the programme.
- **CHB IT 027 IP Telephony and Call recording** – Funding has been provisioned for the project thus lowering the likelihood. The risk will now be revaluated with respect to the delivery of the programme.
- **CHB IT 029 2020 Contract Planning and Procurement Funding** – Funding has been provisioned for the project thus lowering the likelihood. The risk will now be revaluated with respect to the delivery of the programme
- **CHB IT 020 PSN Compliance –** Following remedial actions the Corporation have been granted the PSN Compliance Certificate for a further year.

The current headline figures for the identified risks in the Division are:
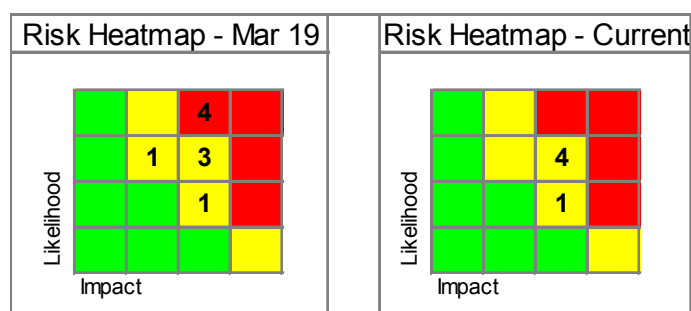
8. **Further breakdown of current Division risks:**

Major Impact:

Risks with "likely" likelihood and "major" impact:	0	⬇
Risks with "possible" likelihood and "major" impact:	3	⬌
Risks with "Unlikely" likelihood and "major" impact:	1	⬌

Serious Impact:

Risks with "likely" likelihood and "serious" impact:	0	⬌
Risks with "possible" likelihood and "serious" impact:	0	⬇
Risks with "unlikely" likelihood and "serious" impact:	1	⬆

⬆	Increase in No.
⬇	Decrease in No.
⬌	Static No.
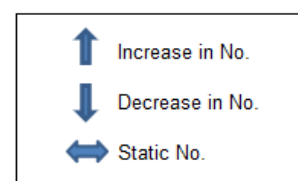
9. Next steps

- Ensuring that IT deal with Risks in a dynamic manner.

- Ensuring all actions are up to date and allocated to the correct responsible owners.

- Ensuring all members of the IT division including suppliers are aware of how Risk is managed within the Corporation and have a mechanism to highlight areas of concern across the estate.

- IT management processes, including Change Management, Problem Management, Continuous Improvement and Incident Management will all now reference or identify risk to ensure that Division risks are identified, updated and assessed on an ongoing basis, so the Risk register remains a live system, rather than a periodically updated record.

Samantha Kay
IT Business Manager
E: samantha.kay@cityoflondon.gov.uk
T: 07817 411176

Appendix A – Information Management Risk

Risk no, title, creation date, owner	Risk Description (Cause, Event, Impact)	Current Risk Rating & Score		Risk Update and date of update	Target Risk Rating & Score		Target Date	Current Risk score change indicator
CR29 Information Management 08-Apr-2019 Peter Kane	**Cause:** Lack of officer commitment and investment of the right resources into organisational information management systems and culture. **Event:** The City Corporation's IM Strategy (2018-2023) is not fully and effectively implemented **Effect:** • Not being able to use relevant information to draw insights and intelligence and support good decision-making • Vulnerability to personal data and other information rights breaches and non-compliance with possible ICO fines or other legal action • Waste of resources storing information beyond usefulness		12	The Information Management strategy has been agreed subject to a more detailed action plan and metrics to track performance. We need to ensure that the IM Strategy is now delivered through a series of actions and activities as detailed below. The actions identified below are Year 1 actions. Actions in subsequent years will be prioritised to ensure full implementation of the strategy. **08 Apr 2019**		6	31-Mar-2020	 Constant

Action no	Action description	Latest Note	Action owner	Latest Note Date	Due Date
CR29a	Ensure that CoL has the necessary awareness, tools and, skills to manage information effectively	Work with the Head of Communications to communicate/raise awareness the IM Strategy and Policies. Provide training in SharePoint in preparation for migrating the Shared drives. Implement protective marking and information classification in CoL. Sharepoint to become the Corporate document management solution.	Sean Green	08-Apr-2019	30-Sep-2019
CR29b	Start the culture change by Integrating good information management practice into the Leadership and	HR to work with the IT and the Corporate Strategy and Performance teams to identify the key skills required for good information management. HR to then develop the training to support this.	Chrissie Morgan	08-Apr-2019	31-Mar-2020

	Management stand of the City of London Learning Academy	HR to review where in HR policies and procedures this can be integrated. HR to Work with the senior leadership team to develop a plan and then deliver key messages and communications on the importance, relevance and benefits of good information management.			
CR29c	Ensure that CoL's information estate is safe, relevant, accurate, reliable, used and trusted.	Implement and communicate relevant IM policies and IM Security. Develop and agree a Data Retention policy that links in with departmental retention schedules taking advice from the LMA.	Sean Green	08-Apr-2019	30-Jun-2019
CR29d	Ensure that CoL's derives real value and benefits from the use of information, data, analysis and modelling	IT to deliver the Business Intelligence Infrastructure to ensure that the Corporate Strategy and Performance team have the tools to develop business intelligence reports and analytics to support better decision making across CoL.	Sean Green/Kate Smith	08-Apr-2019	30-Aug-2019
CR29e	Ensure officers can implement the data retention policy and data discovery requirements from GDPR	The Digital Services Task and Finish group to be established to provide governance and assurance that the strategy is being delivered. New IM Policies and compliance are already governed via the IM Governance Board.	Sean Green; Kate Smith	08-Apr-2019	30- May-2019
CR29f	Ensure officers can implement the data retention policy and data discovery requirements from GDPR	Put in place a new Data retention and discovery toolset to ensure we only retain and archive information in line with the agreed policy and retention schedule	Sean Green	08-Apr-2019	30-Nov-2019