

Committee(s)	Dated:
Digital Services Sub Committee – For Information	4 th November 2021
Subject: IT Division Risk Update – November 2021	Public
Report of: The Chief Operating Officer	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 4 risks. There is currently one Corporate RED risk and one Departmental Red risk. There are no extreme impact risks, there are 4 major impact, and no Serious or Minor impact risks.

IT currently holds 2 risks on the Corporate Risk Register and 2 risks on the Departmental risk register

Summary of the Corporate Risks

CR 16 – Information Security

- We are seeing regular malware being delivered by email every week which is not being captured by the current security products. We have had agreement to upgrade our MS Licences from E3 to E5 which will help mitigate this.
- The Results of the IT Health Check have been received and a Remediation Action Plan (RAP) has been developed. Remediation activities have commenced.
- Work on a simulated cyber-attack is being planned with the IT Security Team for completion by the end of the calendar year.

This is a dynamic risk area and whilst the maturity of 4 is the target, the control scores will go down as well as up as threats, risks and vulnerabilities change.

CR 29 – Information Management

- New business intelligence dashboards continue to be developed for improved decision making by the Corporate Strategy and Performance team
- An updated An Information Management Asset register has been populated for the organisation.
- Plans are being developed for moving unstructured data from Shared Drives to SharePoint is being developed

- There is no dedicated resources to support Information Management and data analysis in the organisation. Unless resourcing is reviewed under the new TOM this situation will not change

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 of Departmental Risks

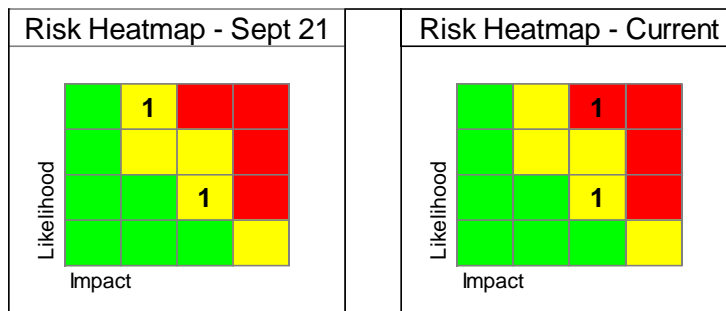
2. The IT Division currently holds 2 Departmental risks, one of which is scored as Red. All risks have owners, clear actions, with target dates to enable focussed management, tracking and regular and consistent reviews.
3. These risks are as follows:
 - CHB IT 004 Business Continuity – Amber
 - CHB IT 031 IT Revenue Budget - Red

Note: details can be reviewed in the appendix.

Current status

4. Since the last report, the IT Risk Register has been closely monitored and actions have been completed to continue the work to mitigate the risks, however, there has been no movement of scores in this period.

The current headline figures for the identified risks in the Division are:



Movement of Risks

Following constant review there has been an increase in the risk scoring of one Corporate and One Departmental Risk since the last report.

- CR 16 – Information Security – This risk increased in likelihood following the increase in Malware attacks that are not being intercepted but the current security products.
- CHB IT 031 IT Revenue Budget – This risk increased in impact from Serious to Major, following a deeper scrutiny of the revenue budget and the reality of the savings targets being met

5. Further breakdown of current Departmental risks:

Major Impact:

	Trend		
Risks with "likely" likelihood and "major" impact:	0	1	↑
Risks with "possible" likelihood and "major" impact:	0	0	↔
Risks with "Unlikely" likelihood and "major" impact:	1	1	↔

↑ Increase in No.

↓ Decrease in No.

↔ Static No.

Serious Impact:

Risks with "likely" likelihood and "serious" impact:	1	0	↓
Risks with "possible" likelihood and "serious" impact:	0	0	↔
Risks with "unlikely" likelihood and "serious" impact:	0	0	↔

6. 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.
- The work detailed above ensures that the Risk register remains a live system, rather than a periodically updated record.

Samantha Kay

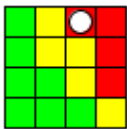
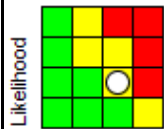

IT Business Manager

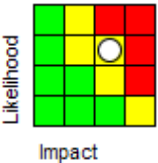
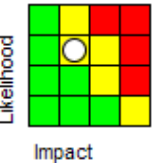

E: samantha.kay@cityoflondon.gov.uk

T: 07817 411176

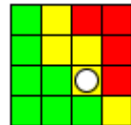


APPENDIX A - CHB IT All CORPORATE & DEPARTMENTAL risks



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/Risk Approach	Current Risk score change indicator
CR16 Information Security (formerly CHB IT 030) 10-May-2019 Emma Moore	Cause: Breach of IT Systems resulting in unauthorised access to data by internal or external sources. Officer/ Member mishandling of information. Event: The City Corporation does not adequately prepare, maintain robust (and where appropriate improve) effective IT security systems and procedures. Effect: Failure of all or part of the IT Infrastructure, with associated business systems failures. Harm to individuals, a breach of legislation such as the Data Protection Act 2018. Incur a monetary penalty of up to €20M. Compliance enforcement action. Corruption of data. Reputational damage to Corporation as effective body.	 Likelihood	16 Impact	. We are seeing regular malware being delivered by email every week which is not being captured by the current security products. We have had agreement to upgrade our MS licences from E3 to E5 which will help mitigate this. . The Results of the IT Health Check have been received and a Remediation Action Plan (RAP) has been developed. Remediation activities have commenced. . Work on a simulated cyber attack is being planned with the IT Security Team for completion by the end of the calendar year. 18 Oct 2021	 Likelihood	8	31-Mar-2022	 Constant

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/Risk Approach	Current Risk score change indicator
CR29 Information Management 08-Apr-2019 John Barradell	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: <ul style="list-style-type: none"> • 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	New business intelligence dashboards continue to be developed for improved decision making by the Corporate Strategy and Performance team • An updated An Information Management Asset register has been populated for the organisation. Plan being developed for moving unstructured data from Shared Drives to Sharepoint is being developed There is no dedicated resources to support Information Management and data analysis in the organisation. Unless resourcing is reviewed under the new TOM this situation will not change 18 Oct 2021		6	31-Dec-2021	 Constant
							Reduce	

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/Risk Approach	Current Risk score change indicator
CHB IT 031 IT Revenue Budget 								

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/Risk Approach	Current Risk score change indicator
CHB IT 004 Business Continuity 30-Mar-2017 Sean Green	Cause: A lack of robust infrastructure and restore procedures are not in place on aging infrastructure. Secondly, there is a lack of resilient or reliable Power services or Uninterruptable Power Supply (UPS) provision in multiple Comms rooms and datacentres in COL and COLP buildings. Event: The IT Division cannot provide assurance of availability or timely restoration of core business services in the event of a DR incident or system failure. There will be intermittent power outages of varying durations affecting these areas/buildings. Effect: The disaster recovery response of the IT Division is unlikely to meet the needs of COL leading to significant business interruption and serious operational difficulties. <ul style="list-style-type: none"> • Essential/critical Systems or information services are unavailable for an unacceptable amount of time • Recovery of failed services takes longer than planned • Adverse user/member comments/feedback • Adverse impact on the reputation of the IT division/Chamberlain's Department 	 Likelihood Impact	8	All services have now been migrated into Azure. Agilisys BC/DR plan has now been provided and is being reviewed internally and will form the basis of the COL IT BCDR Plan. The GW5 has been sent for approval, the project is poised to start immediately. 18 Oct 2021	 Likelihood Impact	4	31-Oct-2021	 Constant

