

Committee(s)	Dated:
Digital Services Sub Committee – For Information	28 th January 2022
Subject: IT Division Risk Update	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 upgraded our MS licences from E3 to E5 which will help mitigate this.
- We are currently working on mitigating a vulnerability recognised worldwide called Logi4j. So far, the major risks of this are contained as we work through the remediation and patching plan.
- Other mitigations include promoting security training and on-going and regular security communications to all staff and Members.
- 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 February 2022.
- Further, IT Security training offered to staff and Members and regular communication on security issues on the intranet and via email

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 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
- The Executive Board has agreed to allow one member of staff to represent each department up to 1 day a week to support IM Projects.

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

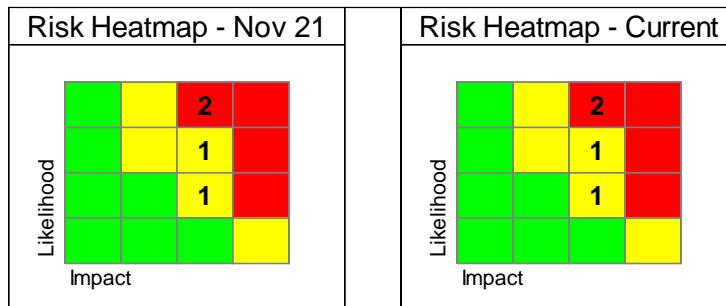
2. The IT Division currently holds 2 Departmental risks, one of which is scored as Red. All risks have owners, clear actions, with target dates to enable focussed management, tracking and regular and consistent reviews.
3. These risks are as follows:
 - CHB IT 004 Business Continuity – Amber – there is a draft BCDR plan which should be finalised by the date of the next DSSC meeting.
 - CHB IT 031 IT Revenue Budget – Red – the IT operating budget is forecast to be overspent at the end of the current financial year.

Note: details can be reviewed in the appendix.

Current status

- 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

- There has been no movement of the risk scores since the last report.

5. Further breakdown of current Departmental risks:

			Trend	
Extreme Impact:				
Risks with "likely" likelihood and "extreme" impact:	0	0	↔	<div><div>↑</div> Increase in No.</div> <div><div>↓</div> Decrease in No.</div> <div><div>↔</div> Static No.</div>
Risks with "unlikely" likelihood and "extreme" impact:	0	0	↔	
Risks with "rare" likelihood and "extreme" impact:	0	0	↔	
Major Impact:				
Risks with "likely" likelihood and "major" impact:	2	2	↔	
Risks with "possible" likelihood and "major" impact:	1	1	↔	
Risks with "Unlikely" likelihood and "major" impact:	1	1	↔	

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)	<p>Cause: Breach of IT Systems resulting in unauthorised access to data by internal or external sources. Officer/ Member mishandling of information.</p> <p>Event: The City Corporation does not adequately prepare, maintain robust (and where appropriate improve) effective IT security systems and procedures.</p> <p>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.</p>	<p>Likelihood</p> <p>Impact</p>	16	<p>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.</p> <p>We are currently working on mitigating a vulnerability recognised worldwide called Logi4j. So far, the major risks of this are contained as we work through the remediation and patching plan.</p>	<p>Likelihood</p> <p>Impact</p>	8	31-Mar-2022	

10-May-2019 Emma Moore				<p>Other mitigations include promoting security training and on-going and regular security communications to all staff and Members.</p> <p>The Results of the IT Health Check have been received and a Remediation Action Plan (RAP) has been developed. Remediation activities have commenced.</p> <p>Work on a simulated cyber attack is being planned with the IT Security Team for completion by the end February 2022.</p> <p>Further, IT Security training offered to staff and Members and regular communication on security issues on the intranet and via email</p> <p>12 Jan 2022</p>				Reduce	Constant
---------------------------	--	--	--	--	--	--	--	--------	----------

Action no	Action description	Latest Note	Action owner	Latest Note Date	Due Date
CR16k	Final stages of completing information security projects which will mean that we can assure Members that the City of London Corporation has implemented all the national government recommended security practices and technology achieving a maturity level of 4.	With the agreement of the E5 business case by Members the improvements to our security stance can now begin with resources procured to support implementation	Gary Brailsford-Hart	12-Jan-2022	31-Mar-2022
CR16m	Work on a simulated cyber attack is being planned with the IT Security Team	<p>The COLP IMS Team are developing and will implement two activities toward the end of the calendar year:</p> <p>A Red Play activity – A scenario-based exercise which simulates a Ransomware attack and tests our response to a similar incident. Scheduled for January 2022, with follow up by the end of the month.</p>	Matt Gosden	12-Jan-2022	28-Feb-2022



CR16n	Work on a simulated cyber attack is being planned with the IT Security Team	A White Hat activity – this is where we employ an Ethical Hacker to try to gain access to COL systems using typical hacking tools and techniques.	Gary Brailsford-Hart	12-Jan-2022	31-Mar-2022
CR16o	Remediation of PSN outstanding issues	PSN submission signed by the town Clerk and document set submitted to the Cabinet Office PSN Assessment Team on Tuesday 11th Jan 2022.	Matt Gosden	12-Jan-2022	30-Mar-2022

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 	 Likelihood Impact	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 The Executive Board has agreed to allow one member of staff to represent each department up to 1 day a week to support IM Projects. There is no Capital investment to improve our IM infrastructure and uncertainty where data analysis responsibilities are to be established in the new TOM. 12 Jan 2022	 Likelihood Impact	6	30-Jun-2022	 Constant
							Reduce	

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	New Information Management Campaign being deployed in January. Work on the role of IM in the new TOM has begun recommended along with a funding bid.	Sean Green	12-Jan-2022	31-Jan-2022
CR29f	Ensure officers can implement the data retention policy and data discovery requirements from GDPR	Reviewing Azure tools that can assist in the analysis of SQL databases	Adam Fielder	12-Jan-2022	31-Jan-2022

CR29g	IM Audit Actions to be implemented	Several audit actions now need to be considered and planned for implementation up to the end of June. Dependent on a resource uplift bid within the IT TOM proposal.	Sean Green	12-Jan-2022	30-Jun-2022
CR29h	W Drive moved to SharePoint	Work to begin on migrating the W Shared Drive to SharePoint following sign off from Executive Leadership team		12-Jan-2022	30-Apr-2022
CR29i	Local SIRO training for the Chief Officer Team	Training to be sourced and provided to all Chief Officers on the responsibilities of a SIRO	Nick Senior	12-Jan-2022	30-Apr-2022
CR29j	IM Maturity Plan	More detailed mitigation actions for cultural, infrastructure and information tooling to be developed – this is resource dependent and will not start till after the new TOM is implemented in April 2022	Sean Green	12-Jan-2022	30-Jun-2022

CHB IT 031b	Prepare and execute the IT savings plan for 21/22 with agreement from relevant stakeholders in the organisation	<p>An interim new dedicated Project Manager and Capacity Manager is being employed to develop and drive forward the IT savings for the Corporation. This is profiled and is being discussed at monthly meetings with the Chamberlain.</p> <p>Ongoing- review process as part of bi-lateral</p>	Sean Green	12-Jan-2022	31-Mar-2022
-------------	---	--	------------	-------------	-------------

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	The draft BCDR plan has been produced but requires further input relating to Critical Apps and Services and the Recovery Point Objective (RPO) and Recovery Time Objective (RTO) to complete. 12 Jan 2022	 Likelihood Impact	4	31-Mar-2022	Constant

Action no	Action description	Latest Note	Action owner	Latest Note Date	Due Date
CHB IT 004k	RPO and RTO of Critical Apps	Find out the RPO/RTOs for all critical applications in Azure and marry back to Critical Apps and Services list	Adam Fielder	12-Jan-2022	31-Mar-2022
CHB IT 004n	Produce IT-wide BC/DR Plan	The first draft of the BCDR Plan has been received but requires further input relating to Critical Apps and Services and the Recovery Point Objective (RPO) and Recovery Time Objective (RTO) to complete. Production is underway and is scheduled for completion by 17th Jan 2022	Matt Gosden	12-Jan-2022	30-Jan-2022
CHB IT 004O	UPS Project Delivery	Following a scheduling delay, the first of three comms rooms will be upgraded on Saturday the 22 nd of January, with the remaining two Comms rooms due for completion by the end of February 2022.	Matt Gosden	12-Jan-2022	28-Feb-2022

