

<b>Committee(s)</b>	<b>Dated:</b>
Digital Services Committee – For Information	4 <sup>th</sup> May 2022
<b>Subject:</b> DITS Risk Update	<b>Public</b>
<b>Report of:</b> The Chief Operating Officer	<b>For Information</b>
<b>Report author:</b> 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 are no RED Risks. There are no extreme impact risks, there are all scored at major impact.

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

- E5 Licences are now implemented for email malware. Further security features are being implemented until June. Further mandatory training to be required during June 2022 for all staff and Members
- Work on a simulated cyber attack is being planned with the IT Security Team for completion by the end of June 2022.
- We have heightened cyber threats with the war in Ukraine with attacks arising from malicious state actors or those sympathetic to those state actors and some near misses. To help further mitigation of this risk we are investigating the options and costs of 24x7 security monitoring with a specialist partner.

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**

- Shared Drive closedown and move to SharePoint completed
- 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.
- New role created to lead on IM in the Digital, Information and Technology Team.

### **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

### **Movement of Risks**

2. The IT Division currently holds 2 Corporate Risks and 2 Departmental risks, none are 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:

#### **Corporate :**

- CR16 – Information Security – This risk has reduced in score from Red (16) to Amber (12) due to the impact being lowered following the successful implementation of the Microsoft E5 Licences
- CR29 – Information Management – This risk has remained at a constant score, however work progresses to close down shared drives and the addition of a new role as part of the DITS TOM implementation

#### **Departmental :**

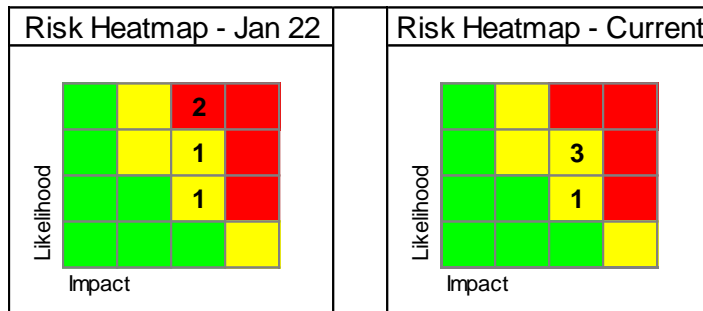
- CHB IT 031 – IT Revenue Budget – This risk has reduced from a Red (16) to Amber (12) due to the likelihood being lowered following the implementation of the DITS TOM. The risk is now at the target score and will be monitored for a few months and will then be deactivated if appropriate
- CHB IT 004 – IT Business Continuity – This risk remains at an Amber (8) and work continues on the DR Planning and UPS implementation.

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:

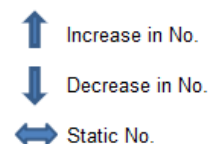


## 5. Further breakdown of current Departmental risks:

### Major Impact:

Risks with "likely" likelihood and "major" impact:	2	0
Risks with "possible" likelihood and "major" impact:	1	3
Risks with "unlikely" likelihood and "major" impact:	1	1

### Trend



### Serious Impact:

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



## 6. Next steps

- IT are holding a risk workshop on 25<sup>th</sup> April to ensure all current risks are captured and relevant.
- 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](mailto: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
CR29 Information Management  08-Apr-2019	<b>Cause:</b> Lack of officer commitment and investment of the right resources into organisational information management systems and culture. <b>Event:</b> The City Corporation's IM Strategy (2018-2023) is not fully and effectively implemented <b>Effect:</b> <ul style="list-style-type: none"> <li>• Not being able to use relevant information to draw insights and intelligence and support good decision-making</li> <li>• Vulnerability to personal data and other information rights breaches and non-compliance with possible ICO fines or other legal action</li> <li>• Waste of resources storing information beyond usefulness</li> </ul>		12	Shared Drive closedown and move to SharePoint completed		6	30-Jun-2022	
				<p>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.</p> <p>There is no Capital investment to improve our IM infrastructure and uncertainty where data analysis responsibilities are to be established in the new TOM.</p> <p>New role created to lead on IM in the Digital, Information and Technology Team</p> <p><b>06 Apr 2022</b></p>				

John Barradell							Reduce	Constant
----------------	--	--	--	--	--	--	--------	----------




Action no	Action description	Latest Note	Action owner	Latest Note Date	Due Date
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	06-Apr-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	Sam Collins	06-Apr-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 – training being delivered during April and May	Nick Senior	06-Apr-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	06-Apr-2022	30-Jun-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
<b>CR16 Information Security (formerly CHB IT 030)</b>	<b>Cause:</b> Breach of IT Systems resulting in unauthorised access to data by internal or external sources. Officer/ Member mishandling of information. <b>Event:</b> The City Corporation does not adequately prepare, maintain robust (and where appropriate improve) effective IT security systems and procedures. <b>Effect:</b> 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 Impact	8	E5 Licences are now implemented for email malware. Further security features are being implemented until June. Further mandatory training to be required during June 2022 for all staff and Members	 Likelihood Impact	6	31-Mar-2023	
				Work on a simulated cyber attack is being planned with the IT Security Team for completion by the end of June 2022.  We have heightened cyber threats with the war in Ukraine with attacks arising from malicious state actors or those sympathetic to those state actors and some near misses. To help further mitigation of this risk we are investigating the options and costs of 24x7 security monitoring with a specialist partner.			Reduce	
10-May-2019 Emma Moore				<b>19 Apr 2022</b>				

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 – Email Malware protection in place – proceeding with further security functional changes enabled by having E5 licence which we will completing by the end of June	Gary Brailsford-Hart	06-Apr-2022	30-Jun-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
<b>CHB IT 004 Business Continuity</b>  30-Mar-2017 Sean Green	<b>Cause:</b> 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. <b>Event:</b> 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. <b>Effect:</b> 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"> <li>• Essential/critical Systems or information services are unavailable for an unacceptable amount of time</li> <li>• Recovery of failed services takes longer than planned</li> <li>• Adverse user/member comments/feedback</li> <li>• Adverse impact on the reputation of the IT division/Chamberlain's Department</li> </ul>	 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) from the Lead Architect to complete and communicate  <b>06 Apr 2022</b>	 Likelihood Impact	4	31-Oct-2021	  Constant





