Committee(s)	Dated:
Digital Services Sub Committee – For Information	12th July 2022
Subject: DITS Risk Update	**Public**
Report of: The Chief Operating Officer	**For Information**
Report author: Samantha Kay – DITS Business Manager	

Summary

All DITS Risks are now in the Risk Management System, with actions included, for the ongoing improvement and continuing assessment to the Management of Risk within DITS.

DITS currently holds 9 risks. There are no RED Risks. There are no extreme impact risks, 5 are currently scored at major impact and 4 at Serious.

DITS currently holds 2 risks on the Corporate Risk Register and 7 risks on the Departmental risk register

Summary of the Corporate Risks

CR 16 – Information Security

Event: The City Corporation does not adequately prepare, maintain robust (and where appropriate improve) effective IT security systems and procedures.

- Update: Microsoft E5 Licence functionality is now implemented for email malware. Further security features are being implemented until the end of June 2022. 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 DITS Security Team.

- DITS have commenced an overarching Security Review, with the aim of reviewing how technology security is managed across the organisation.

CR 29 – Information Management (IM)

Event: The City Corporation's IM Strategy (2018-2023) is not fully and effectively implemented

- There is no Capital investment to improve our IM infrastructure and uncertainty where data analysis responsibilities are to be established in the new TOM.

- W:Drive closedown and move to SharePoint completed

- New role created to lead on IM in the Digital, Information and Technology Service

- Chief Officers being provided with local SIRO training

Recommendation(s)

Members are asked to:
- Note the report.

Main Report

Background

1. Risk remains a key focus for the Digital, Information and Technology Service (DITS), 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 service.

Departmental Risks

2. Following the implementation of the TOM, DITS have reviewed all its Departmental Risks to ensure the current risks are current and relevant to the current environment.

3. One risk was mitigated and reduced to a Service Risk :

   CHB IT 004 – DITS Business Continuity – Following the move to Azure Cloud, upgrading of the UPS devices at key sites, and the ability of the majority of staff being able to work from anywhere (which was tested throughout the pandemic), it was deemed that the likelihood of this risk was reduced. This will now be managed as a Service Level risk.

4. One risk remains on the Departmental Risk Register :

   CHB IT 031 –DITS Revenue Budget – The risk has been redefined, whilst 21/22 saw the risk being focused around the TOM and Fundamental Review saving, the risk now reflects the current situation around Inflation, Recharging and Recruitment costs.

5. Six additional risks have been added to the DITS Departmental Risk Register, all of which are scored as Amber. These are as follows :
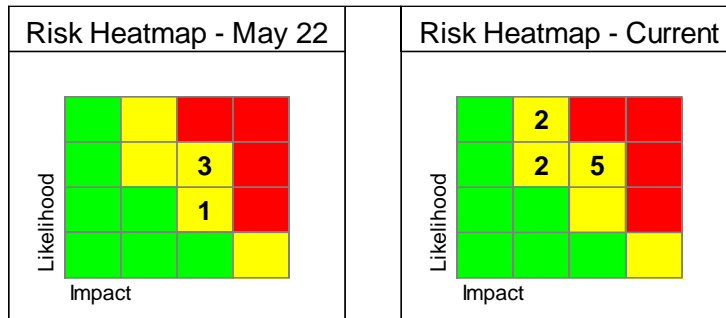
   - **COO DITS 037 Service transition (time)** – Decisions are delayed in regards to Transition of services from expiring contracts.
   - **COO DITS 039 Service transition (quality)** – New technologies and services being introduced are not fit for purpose
   - **COO DITS 040 Resilience and complexity** – Critical services are not sufficiently resilient
   - **COO DITS 034 IT Capacity** – Vacancies within DITS mean there is not enough capacity to maintain services.
   - **COO DITS 035 Recruitment and retention** – Failure to recruit to current and potential, future vacancies in a timely manner
   - **COO DITS 044 Head of profession** - Failure to establish a Head of Profession role in Corporation due to the Director leaving

   Note: details can be reviewed in the appendix.

Current status

6. Since the last report, the DITS Risk Register has been closely monitored and actions have been completed to continue the work to mitigate the risks.

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

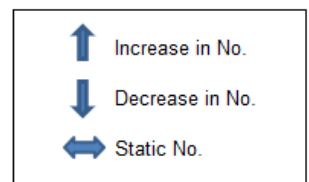7. Further breakdown of current Departmental risks:

Major Impact:			**Trend**
Risks with "likely" likelihood and "major" impact:	0	0	↔
Risks with "possible" likelihood and "major" impact:	2	4	↑
Risks with "Unlikely" likelihood and "major" impact:	1	0	↓
Serious Impact:			
Risks with "likely" likelihood and "serious" impact:	1	4	↑
Risks with "possible" likelihood and "serious" impact:	0	1	↓
Risks with "unlikely" likelihood and "serious" impact:	0	0	↔

↑	Increase in No.
↓	Decrease in No.
↔	Static No.

7. Next steps

- Ensuring that DITS proactively manage Risks.

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

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

- DITS management processes, including Change Management, Problem Management, Continuous Improvement and Incident Management will all now reference or identify risk to ensure that service 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.
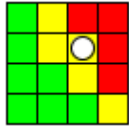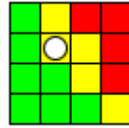
Samantha Kay
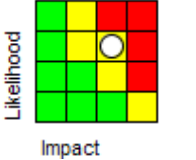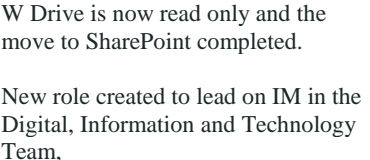DITS Business Manager
E: samantha.kay@cityoflondon.gov.uk
T: 07817 411176

APPENDIX A - CHB IT All CORPORATE & DEPARTMENTAL risks

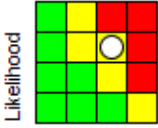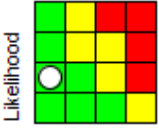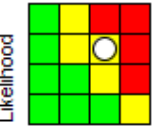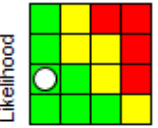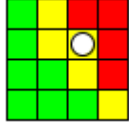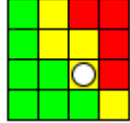| Risk no, title, creation date, owner	Risk Description (Cause, Event, Impact)	Current Risk Rating & Score		Risk Update and date of update	Target Risk Rating & Score		Target Date/Risk Approach	Current Risk score change indicator
CR16 Information Security (formerly CHB IT 030)	**Cause**: Breach of IT 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.		12	E5 Licences are now implemented for email malware. Further security features are being implemented until June 2022. Security enhancements DITs have implemented include: Safelinks for Microsoft Defender – this scans links in incoming emails before the email reaches the recipient, dramatically reducing phishing email and preventing access to infected websites. Multifactor Authentication is now mandatory (by tech policy) for all users of technology services		6	31-Mar-2023	

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
				Guests (external attendees) can no longer automatically join a Teams meeting and must now wait in the virtual lobby before being admitted. DITs have commenced an overarching Security Review, with the aim of reviewing how technology security is managed across the organisation. This will include a RACI across internal and external stakeholders, a review of the processes and tools involved. Ultimately this will produce recommendations for improvements in security management.				
10-May-2019 Emma Moore				**23 Jun 2022**			Reduce	Constant

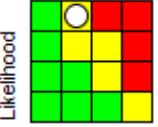| Risk no, title, creation date, owner	Risk Description (Cause, Event, Impact)	Current Risk Rating & Score		Risk Update and date of update	Target Risk Rating & Score		Target Date/Risk Approach	Current Risk score change indicator
CR29 Information Management 08-Apr-2019	**Cause:** Lack of officer commitment 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		12	W Drive is now read only and the move to SharePoint completed. New role created to lead on IM in the Digital, Information and Technology Team, Chief Officers being provided with local SIRO training **23 Jun 2022**		6	31-Dec-2022	▬

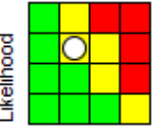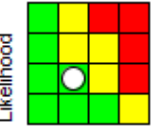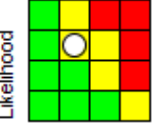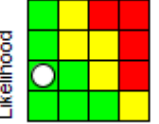| Risk no, title, creation date, owner	Risk Description (Cause, Event, Impact)	Current Risk Rating & Score		Risk Update and date of update	Target Risk Rating & Score		Target Date/Risk Approach	Current Risk score change indicator
John Barradell	• Vulnerability to personal data and other information rights breaches and non-compliance with possible ICO fines or other legal action • Waste of resources storing information beyond usefulness						Reduce	Constant
COO DITS 037 Service transition (time) 19-May-2022 Matt Gosden	**Cause:** Information is not forthcoming, or decisions are not made in a timely fashion, at the appropriate level. **Event:** A consensus on the future critical service elements is not reached, or decisions on these are not made in time to ensure delivery by the end of the current contract. **Effect:** on the future critical service elements is not reached, or decisions on these are not made in time to ensure delivery by the end of the current contract. Further detail is documented in the CPO Risk Register for the programme.		12	A RACI for the design, decision and approval process, alongside a key decision milestone plan should be produced to ensure the right approvals are obtained from the right people at the right time to ensure progress. **23 Jun 2022**		2	31-Aug-2023 Constant	▬

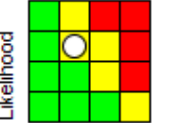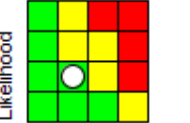| Risk no, title, creation date, owner	Risk Description (Cause, Event, Impact)	Current Risk Rating & Score		Risk Update and date of update	Target Risk Rating & Score		Target Date/Risk Approach	Current Risk score change indicator
COO DITS 039 Service transition (quality) 19-May-2022 Matt Gosden	**Cause:** The new service design (Future Operating Model) is not based on the right information or does not allow for the advancements and investments in technology or processes made by the organisation. **Event:** The future technology service being designed and delivered by the programme does not evolve through the adaptation of the new technology and/or new processes we have, or will have available. **Effect:** The service continues to be sub-optimal during and beyond transition, or the Agilisys contract needs to be extended as-is, rather than driving modernisation and cost reduction. Further detail is documented in the CPO Risk Register.		12	Degradation of service during transition and beyond into the FOM; in customer satisfaction, service availability; contract extensions. **23 Jun 2022**		2	31-Aug-2023	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
COO DITS 040 Resilience and complexity 19-May-2022 Matt Gosden	**Cause**: A lack of end-to-end resilience of critical services remain, or technology areas remain complex. **Event**: There is a major failure in critical parts of the IT infrastructure, which is difficult to avoid, remediate or recover from. **Effect**: Significant incident could lead to an impact to productivity of the business with loss of access to Critical systems. Could lead to financial and reputational impact		12	Although most critical systems are now in the cloud, there remain some elements of our connectivity or technology which remain complex or non-resilient. There is a Business Continuity Plan for IT. The DITs team will plan and deliver a DR test for the next 12 months, consisting of a series of tests of the main areas of risk. **23 Jun 2022**		8	30-Jun-2023	▬ 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
COO DITS 034 IT Capacity 19-May-2022 Sam Collins	*Cause:* The DITS TOM has resulted in several critical vacancies. There has also been two leadership team resignations with the incumbents leaving CoL in June 22. *Event:* It is likely to take 3-6 months to fill vacancies which will need contractors to back-fill where this is authorised. Contractor costs will place additional pressures on the DITS budget *Effect:* Staff in post are more stretched. They experience stress and the DITS team fail to deliver against all their requires priorities and SLA's.	Likelihood / Impact grid	8	Recruitment for all vacancies to be accelerated during June 2022. Monitor stress levels of team and report back to HR Business Partner for mitigating support **23 Jun 2022**	Likelihood / Impact grid	3	31-Oct-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
COO DITS 031 IT Revenue Budget 10-May-2021 Sam Collins	**Cause:** The DITS team has had a revenue budget cut of £2m for 22/23. **Event:** There is on-going pressures on the DITS budget from variable spend on licences, storage and unplanned maintenance. There is also DITS contracts that could be subject to in year inflationary pressure. There are unplanned recruitment costs for several vacancies that will need to be filled. **Effect:.** The DITS budget could be overspent in 2022/23 The services provided by IT to the organisation have already been descoped to achieve the revenue reductions required in this financial year.		6	The DITS budget is monitored monthly with Finance and the COO. DITS are holding some vacancies and will be implementing projects in 22/23 that should reduce revenue spend **23 Jun 2022**		4	31-Mar-2023	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
COO DITS 035 Recruitment and retention 19-May-2022 Sam Collins	Cause: The recent Target Operating Model exercise and ongoing uncertainty within the Division has led to a number of vacant posts and key individuals leaving the organisation. Event: That the Division fails to successfully recruit to the vacant posts and departing staff result in a significant loss of corporate knowledge and expertise Effect: This results in a general loss of capacity, expertise and knowledge within the division, severely limiting the ability of the division to provide a stable and secure IT Service and Key Programmes of work are disrupted or put at risk.		6	3 days a week and getting the right people 23 Jun 2022		2	30-Sep-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
COO DITS 044 Head of profession 20-May-2022 Sam Collins	**Cause:** Failure to establish a Head of Profession role in Corporation due to the Director leaving **Event:** Disparate technology and standards applied across the Corporation **Effect:** Wasted investment, lack of economies of scales and increased cyber threats		**6**	The role needs to influence stakeholders with Digital and Technology responsibilities and apply consistent good practice and standards across the Corporation and Institutions **23 Jun 2022**		**4**	31-Mar-2023	 Constant