

Committee(s)	Dated:
Digital Services Sub Committee – For Information	5 th July 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 4 risks, a reduction of one from the previous period. There are currently no RED risks. There are no extreme impact risks, there are 3 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 - Following review with A&R com and DSSC it was agreed that further steps were required to achieve maturity level that could bring the score to its target

CR 25 – GDPR Regulation Compliance – Will continue to be monitored following the closure of the formal project.

CR 29 – Information Management – The Information Management strategy has been agreed subject to a more detailed action plan and metrics to track performance. Progress is being made in developing a draft retention and disposal policy

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 4 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:
 - 3 Risks have been reduced from Departmental to Divisional level.
 - 1 Risk has increased from Divisional to Departmental level.
 - 1 Risk has been deactivated
 - 2 New risks have been identified

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

Movement of Risks

4. 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 020 – PSN Compliance** – the PSN Compliance certificate was granted, risk will now be monitored a Divisional Level
- **CHB IT 026 – Failure to commence CoLP IT Modernisation** - Following initial funding approval this was reduced to divisional level.
- **CHB IT 029 - 2020 Contract Planning and Procurement** – Following initial funding approval this was reduced to divisional level.

5. Risks increased from Divisional to Departmental Level

- **CHB IT 001 – Resilience – Power & Infrastructure** - following the failure of UPS devices this risk has been increase to departmental level

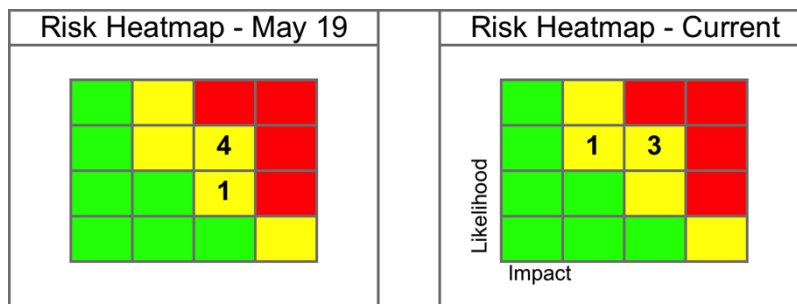
6. Risks that have been deactivated.

- **CHB IT 027 – IP Telephony – Cessation of dependant Service** - following the successful migration and cessation of services this risk has been deactivated.

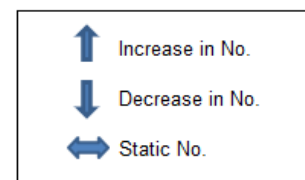
7. New Risks

- **CHB IT 028 – Air-conditioning Failure in Datacentres** – Following the failure of air conditioning units within data centres a new risk was identified due to critical IT systems being at threat.

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	0	↔
Risks with "possible" likelihood and "major" impact:	3	3	↔
Risks with "Unlikely" likelihood and "major" impact:	1	0	↓

Serious Impact:

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

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

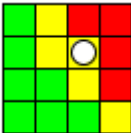
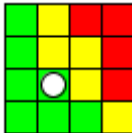
T: 07817 411176

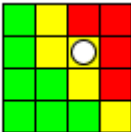
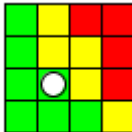
APPENDIX A - CHB IT All DEPARTMENTAL risks

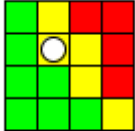
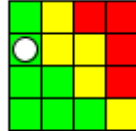



Rows are sorted by Risk Score

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
CHB IT 001 Resilience - Power and infrastructure. 30-Mar-2017 Sean Green	<p>Cause: 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.</p> <p>Event: There will be intermittent power outages of varying durations affecting these areas/buildings.</p> <p>Effect:</p> <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 	 <p>Likelihood</p> <p>Impact</p>	12	<p>Recent failures with UPS equipment have led to this risk being escalated to departmental level.</p> <p>Guildhall has been prioritised as part of audit.</p> <p>Audit on track. Reporting will commence over coming weeks.</p> <p>18 Jun 2019</p>	 <p>Likelihood</p> <p>Impact</p>	2	31-May-2020	 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	Current Risk score change indicator
CHB IT 004 Business Continuity / Disaster Recovery - planning and management. 30-Mar-2017 Sean Green	Cause: A lack of clear understanding of Business need for Services and Applications. No procedure in place for regular reviews with business. 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. Effect: The disaster recovery response of the IT Division is unlikely to meet the needs of COL and COLP leading to significant business interruption and serious operational difficulties.	 Likelihood Impact	12	DR test set for 25th June. With results and lessons learnt paper to be available by 2nd July 14 Jun 2019	 Likelihood Impact	4	15-Sep-2019	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	Current Risk score change indicator
CHB IT 028 Air Conditioning Failure in Datacentres 10-Jun-2019	Cause: The air conditioning units are failing in a number of the Guildhall Communication Equipment Rooms (CER's) / Datacentres. The existing air conditioning units are circa 12 years old and are being reset on a daily basis by the facilities team to keep them functional Event: There will be intermitted / prolonged service disruptions across the IT service provision. Effect: • 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	12	Temporary portable air conditioning unit has been placed in CER. The site assurance audit will produce recommendations on security, management and reliance of all CoL and CoLP comms rooms on a tiered basis. The scope has been increased to include environmental services (air conditioning) 18 Jun 2019	 Likelihood Impact	4	31-Mar-2020	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	Current Risk score change indicator
CHB IT 029 iTrent Contract 18-Jun-2019	Cause: Extension of contract passed the envisaged term of 10 years with no permissible grounds. No projects started to procure a replacement. Event: City of London receive a challenge around the contract for iTrent with MHR Ltd around the exemption of contract. Effect: Legal challenge/court proceedings from a competitor to iTrent. CoL could be forced to issues 18 months termination notice before they are ready to implement a replacement product.	 Likelihood Impact	6	Project planning has commenced 18 Jun 2019	 Likelihood Impact	3	31-Mar-2020	 Constant

Three Corporate risks

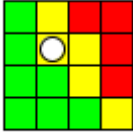
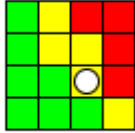

Report Author: Paul Dudley

Generated on 18 June 2019



Rows are sorted by Risk Score

[illegible]

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
CR16 Information Security (formerly CHB IT 030) 10-May-2019 Peter Kane	Cause: Breach of IT Systems resulting in unauthorised access to data by internal or external sources. Officer/ Member mishandling of information. Event: Cybersecurity attack - unauthorised access to COL IT systems. Loss or mishandling of personal or commercial information. 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	6	Following review with A&R committees and DSSC it was agreed that further steps were required to achieve maturity level that could bring the score to its target 14 Jun 2019	 Likelihood	8	31-Oct-2019	 Decreasing

