

Committee(s)	Dated:
Digital Services Sub Committee – For Information	11th September 2020
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. 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.

Summary of the Corporate Risks

CR 16 – Information Security -

- Regular security updates have been provided to relevant people throughout COVID.
- A Gateway paper is currently being drafted for further IT Security Investment.
- Reviewing the National Cyber Security Training with the view to provide training to all staff.
- PSN Accreditation has been approved for a further 12 months.

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 Information Management Awareness campaign has been completed. Second campaign is planned for October
- Work has begun to review relevant staff roles that should have an information management competency added
- An investment Gateway paper has been drafted
- A new Local Information Manager Role is currently being launched into the organisation
- The Technical Pilot for protective marking was completed prior to COVID. Ready for launch at the appropriate time.

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

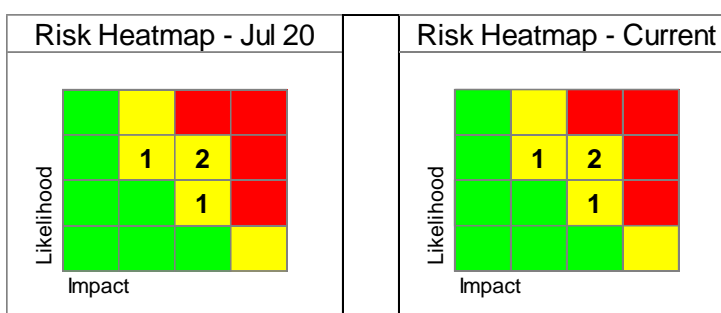
Current Position

2. The IT Division Currently holds 2 Amber risks on the Corporate Risk Register. 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 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:

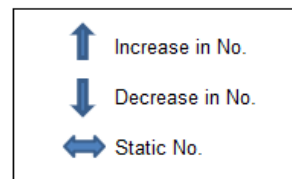


8. Further breakdown of current Division risks:

Major Impact:

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

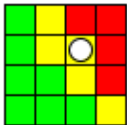


E: samantha.kay@cityoflondon.gov.uk

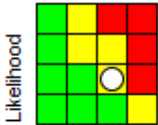
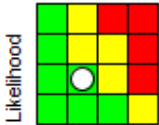

T: 07817 411176




APPENDIX A - CHB IT All 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	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: 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 Impact	12	Regular security updates have been provided to relevant people throughout COVID. A Gateway paper is currently being drafted. Reviewing the National Cyber Security Training with the view to provide training to all staff. PSN remediation activities are complete and have been submitted to the Cabinet Office. 27 Aug 2020	 Likelihood Impact	8	30-Apr-2021	 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
CR29 Information Management 08-Apr-2019 John Barradell	<p>Cause: Lack of officer commitment and investment of the right resources into organisational information management systems and culture.</p> <p>Event: The City Corporation's IM Strategy (2018-2023) is not fully and effectively implemented</p> <p>Effect:</p> <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 	<div> <div>Likelihood</div>  <div>Impact</div> </div>	12	<ul style="list-style-type: none"> • New business intelligence dashboards continue to be developed for improved decision making by the Corporate Strategy and Performance team • An Information Management Awareness campaign has been completed. Second campaign is planned for October • Work has begun to review relevant staff roles that should have an information management competency added • Gateway paper has been drafted • Local Information Manager Role has been launched into the organisation. Individuals have been identified and training will commence in July • The Technical Pilot for protective marking was completed prior to COVID. Ready for launch at appropriate time 27 Aug 2020	<div> <div>Likelihood</div>  <div>Impact</div> </div>	6	31-Jan-2021	 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 Management. 30-Mar-2017 Sean Green	Cause: A lack of robust infrastructure and restore procedures are not in place on aging infrastructure. 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 leading to significant business interruption and serious operational difficulties.	 Likelihood	8	The Azure migration is almost complete. However, some core services remain in IaaS due to incompatibility with Azure. Agilisys have notified COL of their departure from the Datacentre contract at the end of Feb/March 2021, therefore the removal of these services is now time sensitive and critical. 27 Aug 2020	 Likelihood	4	31-Mar-2021	 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 extension 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	6	Soft Market Testing completed with leading ERP Suppliers. Options review to be presented in August. 27 Aug 2020	 Likelihood	3	30-Jun-2021	 Constant