

| | |
|---|------------------------|
| Committee(s) | Dated: |
| Digital Services Sub Committee – For Information | 26th March 2021 |
| 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 3 risks. There are currently no RED risks. There are no extreme impact risks, there are 3 major impact, and no Serious or 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 stakeholders throughout COVID.
- A Gateway paper is currently being drafted for further IT Security Investment.
- All Staff Mandatory Security training is being held in April 21.
- An IT health check has been carried out for the City of London Police with remediations being completed.

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
- Information Management Asset register is being populated for the organisation.
- Plan being developed for moving unstructured data from Shared Drives to SharePoint

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

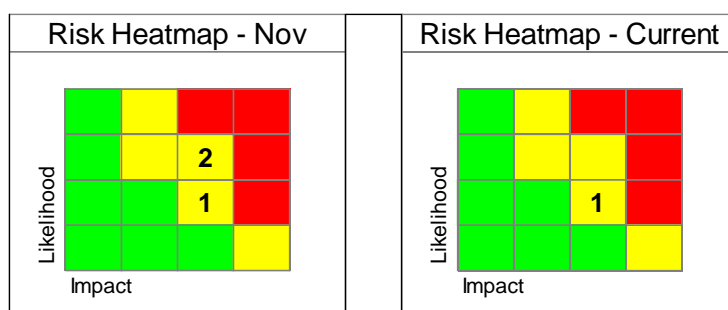
Current Position

2. The IT Division Currently holds 2 Amber risks on the Corporate Risk Register. The IT Division currently holds 1 risk, which is not 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:



Movement of Risks

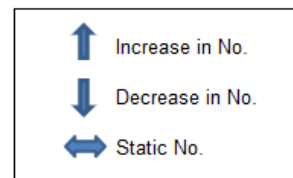
4. Since the last report two risks have been mitigated from the IT Department risk register details of these are as follows:

CHB IT 030 2020 - Managed Service Contract – the new 2020 Managed Service Contract with Agilisys went live on 1st January 2020, reducing the risk from Departments to Service Level, the delivery of this contract will be monitored as a Service Level Risk for the foreseeable future.

CHB IT 001 Resilience - Power and infrastructure. – following the migration of services to the Azure Platform, including CBIS and Spatial Applications these has enabled the risk to be reduced from Departmental to Service level, this will now be monitored as such for the foreseeable future.

5. Further breakdown of current Division risks:

| Major Impact: | | | Trend |
|--|---|---|-------|
| Risks with "likely" likelihood and "major" impact: | 0 | 0 | ↔ |
| Risks with "possible" likelihood and "major" impact: | 2 | 0 | ↓ |
| Risks with "Unlikely" likelihood and "major" impact: | 0 | 0 | ↔ |
| 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 | ↔ |



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

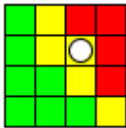
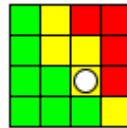

IT Business Manager

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) 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. All Staff Mandatory Security training to be held in March. Submitted to the Cabinet Office. 07 Mar 2021 |  Likelihood Impact | 8 | 30-Jun-2021 |  Constant |
| | | | | | | | Reduce | |

