Committee(s)	**Dated:**
IT Sub-Committee – For Information	24th November 2017
Subject: IT Division Risk Update	
Report of: The Chamberlain	**For Information**
Report author: Samantha Kay – IT Business Manager	

NOT FOR PUBLICATION

By virtue of paragraph [insert exemption clause as per separate guidance] of Part 1 of Schedule 12A of the Local Government Act 1972

Summary

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

- All the IT risks are now being tracked in the corporate risk management system Covalent.

- The IT Division currently holds 17 risks, of which 2 are RED. These risks are tracked in Covalent.

- There are no extreme impact risks, there are 9 major impact and 8 serious impact risks.

- The two Red risks are being addressed and reviewed as part of the Transformation Programme. This has been reduced by one due to mitigation work carried out by the remote site remediation work.

- Periodic review meetings are being held with the relevant IT staff to ensure all risks are managed and reviewed in a timely manner.

Summary of Red Risks

- CHB IT 001 – Resilience – Power & Infrastructure - IT Division and partners cannot effectively deliver reliable, resilient IT services to meet the business needs due to insufficient/unsound power and infrastructure across the estate.

- CHB IT 003 – End to End System monitoring & alerting - The IT team are not able to provide assurance that key infrastructure, networks or services are monitored adequately, with correctly configured alerts in place.

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 drives the priority for project works and Change Management decisions. Regular reviews will ensure the ongoing successful management of these risks.

Current Position

2. Following further assessment, the IT Division currently holds 17 risks, of which 2 are RED. One of which is both a Division Risk and a Department Risk. These risks are all tracked in Covalent.

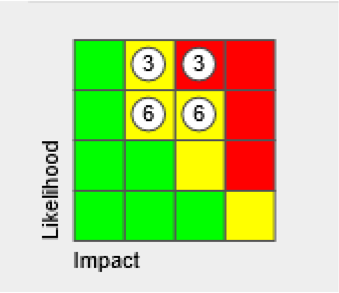
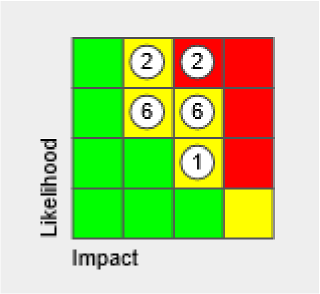
3. All risks have owners, clear actions, with target dates to enable focussed management, tracking and regular and consistent reviews.

Current status

4. This period there has been movement on three of the risks, the remainder continue to be monitored alongside the relevant on-going projects.

   - CHB IT 002 – Connectivity - Red downgraded to amber, following the completion of the site remediation across the Corporation, it was deemed that this preliminary work has mitigated the immediate risk to the sites connectivity providing better knowledge of all sites and increased security around the network provision.
   - CHB IT 015 – Change Control – due to implementation of new change control process, the likelihood of a change not being managed appropriately has been reduced
   - CHB IT 011 - Service outage – was removed from the IT register following a review which confirmed that all aspects of this risk were covered by a risk at corporate level, therefore this is risk has been superseded by CR19.

5. The current headline figures for the identified risks in the Division are:

Risk heatmap – Sept	Risk heatmap – Current
	

Further breakdown of current Division risks:

Extreme Impact:

Risks with "likely" likelihood and "extreme" impact:	0	⇔
Risks with "unlikely" likelihood and "extreme" impact:	0	⇔
Risks with "rare" likelihood and "extreme" impact:	0	⇔

Major Impact:

Risks with "likely" likelihood and "major" impact:	2	↓
Risks with "possible" likelihood and "major" impact:	6	⇔
Risks with "Unlikely" likelihood and "major" impact:	1	↑

Serious Impact:

Risks with "likely" likelihood and "serious" impact:	2	↓
Risks with "possible" likelihood and "serious" impact:	6	⇔

Analysis of the Division risk position

6. Division risks have lowered to 17 due to the removal of the IT Service Outage risk. This risk is now discussed as a matter of course ensuring any potential risks are highlighted and discussed and added to the register as necessary.

7. 2 risks remain as RED currently, with no RED risks scoring higher than 16. One risk was reduced from Red to Amber due to completion of the remote site remediation work. Mitigating actions on the remaining red risks will be delivered through the changes and activities already planned with the IT Transformation

Programme. Actions are in place to reduce the likelihood and impact of these risks as transformation progresses. (See appendix 1)

8. These risks will be monitored and managed alongside the Transformation programme to ensure that the activities will mitigate the risks as anticipated.

9. Improved Management of Risk processes and more involvement and knowledge from across IT will continue to produce further re-assessment as a consensus of the risks and actions are developed.

10. Two live issues – PSN and IR35 – are currently being actively managed. In future a more agile approach will be adopted to framing risks around issues such as this as they emerge.

Next steps

11. 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.

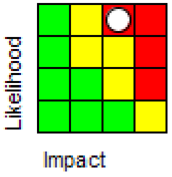
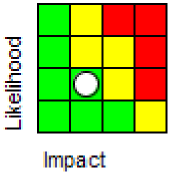
12. IT management processes, including Change Management, Problem Management, Continuous Improvement and Incident Management will all now reference or identify risk to ensure that Division risks are identified, updated and assessed on an ongoing basis, so the Risk register remains a live system, rather than a periodically updated record.

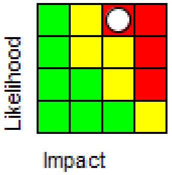
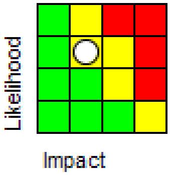
Appendices

- Appendix 1 – High level summary of current RED risks.

Samantha Kay
IT Business Manager
E: samantha.kay@cityoflondon.gov.uk
T: 07817 411176

Appendix 1: High level summary of current RED 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
CHB IT 001 Resilience - Power and infrastructure. 30-Mar-2017 Sean Green	**Cause:** A lack of resilient or reliable Power services, or Uninterruptable Power Supply (UPS) provision in multiple Communications rooms and datacentres in COL and COLP buildings. An aged power infrastructure with multiple Single Points of Failure. Unclear demarcation of responsibilities or communication around Change Management or maintenance of power. **Event:** IT Division and partners cannot effectively deliver reliable, resilient IT services to meet the business needs. **Effect:** Inability to meet current or future IT service needs. Systems or information services are unavailable due to a power related incident. Recovery of failed services takes longer.		**16**	The in-flight Network Transformation programme will deliver improved communications room cabling and infrastructure, updated policies, documentation, management processes and support provision. A project to remediate power, cabling and secure housing of utilities and services across all sites is now coming to an end on the Corporation site, Police sites have commenced. This work has prepared the sites for the implementation of the new network. A new policy and ToR including roles and responsibilities will be agreed with City Surveyors, including demarcation of responsibilities, Change Control and communication. **23 Oct 2017**		**4**	31-Dec-2017	▬

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 003 End-to-end System monitoring and alerting 05-Jun-2017	**Cause:** End-to-end IT systems are not being monitored or alerted effectively. **Event:** The IT team are not able to provide assurance that key infrastructure, networks or services are monitored adequately, with correctly configured alerts in place. **Effect:** The IT team are not aware of issues with the infrastructure, services or connectivity until they become an outage leading to a decreased in confidence in the IT function. Longer incident analysis/diagnosis and resolution times resulting in unsatisfactory service outages. A decreased ability to recognise adverse behaviours such as broadcast storms or security breaches.		**16**	Transformation Programme will deliver a new infrastructure and improved Configuration Management processes, ensuring each new piece of equipment will be added to the monitoring tool, with appropriate alerting and the Configuration Management Database and removed when no longer in service. This will also enable improved monitoring of components during and after a change **23 Oct 2017**		**6**	31-Dec-2017	▬