Committee(s)	**Dated:**
Digital Services Sub Committee – For Information	3rd September 2021
Subject: IT Corporate Risks and Risk Appetite Deep Dive	**Public**
Report of: The Chief Operating Officer	**For Decision**
Report author: Sean Green – IT Director	

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.

IT currently holds 2 risks on the Corporate Risk Register and 2 risks on the departmental risk register.

The City of London Corporation (CoLC) has a Risk Management Policy and Strategy that was reviewed and endorsed by the Audit and Risk Committee in May 2021.

The Digital Services Sub Committee have determined that they would like to review the two critical corporate IT risks in the context of risk appetite. This deep dive reviews the methodology for risk appetite and the two corporate risks in the context of a suggested risk appetite statement.

The approach to the determining risk appetite has been informed by the CoLC Risk Management Policy and Strategy and the City of London Risk Appetite Statement.

Recommendation(s)

Members are asked to:

- Note the report and agree a statement that describes their risk appetite as a committee to guide the IT Director and his team in the treatment of Information and Security risks.

Main Report

Background

1. CoLC is responsible for ensuring that its business is conducted in accordance with the law and proper standards of governance; that public money is safeguarded and properly accounted for, and used economically, efficiently and effectively; and that arrangements are made to secure continuous improvement in the way its functions are operated.

2. In discharging this overall responsibility, CoLC is responsible for putting in place proper arrangements for the governance of its affairs and facilitating the effective exercise of its functions, which includes arrangements for the management of risk.

3. The Digital Services Sub Committee (DSSC) have been actively involved in reviewing and scrutinising the critical IT Corporate and Departmental risks providing for the last 5 years providing challenge and supporting mitigating actions most notably with the ongoing investment and oversight required for CR16 the IT Security risk.

4. The IT Division currently holds 2 corporate risks, which are not scored as Red. All risks have owners, clear actions, with target dates to enable focussed management, tracking and regular and consistent reviews.

5. The number of IT risks has increased over the last 12 months from 6 to 10 see Appendix A.

6. This report is a deep dive to help DSSC review two corporate risks that the committee monitor in the context of risk appetite.

Risk Appetite

7. When considering threats, risk appetite involves assessing the level of exposure that can be justified and tolerated by comparing the cost (financial or otherwise) of mitigating the risk with the cost of the exposure if the risk crystallises into an issue and finding an acceptable balance.

8. Target risk **–** The risk score that the organisation wishes to reduce the risk to (i.e., target risk score) after the completion of all related actions and achieved by a certain date.

9. Risk Appetite: the level of risk with which an organisation aims to operate.

10. The benefits of adopting a risk appetite include:

    - Supporting informed decision-making;
    - Reducing uncertainty;
    - Improving consistency across governance mechanisms and decision-making;
    - Supporting performance improvement;
    - Focusing on priority areas within an organisation; and
    - Informing spending review and resource prioritisation processes.

11. Description of Risk Appetite Levels

Appetite Levels	Description
Averse (Low)	Avoidance of risk and uncertainty is a key objective.
Minimalist (Medium-Low)	Preference for ultra-safe options that have a low degree of inherent risk and only have a potential for limited reward.
Cautious (Medium)	Preference for safe options that have a low degree of residual risks and may only have limited potential for reward.
Open (Medium-High)	Willing to consider all options and choose the one that is most likely to result in successful delivery while also providing an acceptable level of reward.
Hungry (High)	Eager to be innovative and to choose options based on potential higher rewards (despite greater inherent risk).

Implications

12. The level of the risk appetite provides specific guidance officers, project owners and risk owners.

13. Risk appetite indicates to risk owners the extent to which they need to mitigate risks.

14. Risk appetite guides risk owners in the organisation; to whom the risks may be escalated to and, in the types and levels of risk they can accept on behalf of the organisation.

15. Risk appetite maps to a maximum level of residual risk that can be accepted on behalf of CoLC at each level in the risk management chain. (See tables below).

Residual Risk Level	Risk appetite				
	Risk Averse	Minimalist	Cautious	Open	Hungry
Green	CISO	IAO	IAO	IAO	IAO
Amber	CISO	CISO	CISO	IAO	IAO
Red	SIRO	SIRO	SIRO	SIRO	CISO

Residual Risk Level	Risk appetite				
	Risk Averse	Minimalist	Cautious	Open	Hungry
Very Low	IRO	IAO	IAO	IAO	IAO
Low	SIRO	IRO	IAO	IAO	IAO
Medium	SIRO	CISO	IRO	IAO	IAO
Medium-High	SIRO	SIRO	CISO	IRO	IAO
High	SIRO	SIRO	SIRO	SIRO	IRO/CISO
Very High	SIRO	SIRO	SIRO	SIRO	CISO

16. Key themes for risks that this committee are responsible for:

    - Technology risks – Risks arising from technology not delivering the expected services due to inadequate or deficient system/process development and performance or inadequate resilience.

    - Information risks – Risks arising from a failure to produce robust, suitable and appropriate data/information and to exploit data/information to its full potential.

    - Security risks – Risks arising from a failure to prevent unauthorised and/or inappropriate access to key government systems and assets, including people, platforms, information and resources. This encompasses the subset of cyber security.

    - Project/Programme risks – Risks that change programmes and projects are not aligned with strategic priorities and do not successfully and safely deliver requirements and intended benefits to time, cost and quality.

    - Reputational risks – Risks arising from adverse events, including ethical violations, a lack of sustainability, systemic or repeated failures or poor quality or a lack of innovation, leading to damages to reputation and or destruction of trust and relations.

Suggested Risk Position of IT Security and Information Management Risks (See Appendix B)

17. DSSC has a low to moderate appetite in relation to technology and information risk. This risk appetite applies to both the CoLC's' technology networks; cloud-based applications used to support delivery of services; and processes where manual documents are used and retained.

18. This risk appetite will vary depending on the nature; significance; and criticality of systems used, and the services that they support.

19. Target risk is managed through ongoing use of inbuilt technology security controls such as user access; encryption; data loss prevention; firewalls; and ongoing vulnerability scanning and a range of technology security protocols and procedures.

20. CoLC is now progressing towards full alignment to 'Best' recommendations from the National Cyber Security Centre for Cyber resilience with the implementation of Microsoft E5 licences.

21. Directors and Officers are responsible for ensuring ongoing compliance with technology security protocols, policies, standards and procedures.

Next steps

22. Review or amend and then adopt the risk appetite statement in this report as a guidance for Director of IT and his team.

23. Ensure that IT continue to deal with Risks in a dynamic manner

24. Continue to seek assurance that IT management processes, including Change Management, Problem Management, Continuous Improvement and Incident Management will all reference or identify risk to ensure that Division risks are identified, updated and assessed on an ongoing basis.

25. Note that the risk appetite statement for Officers is being reviewed by the new Executive Leadership Board in October 2021.

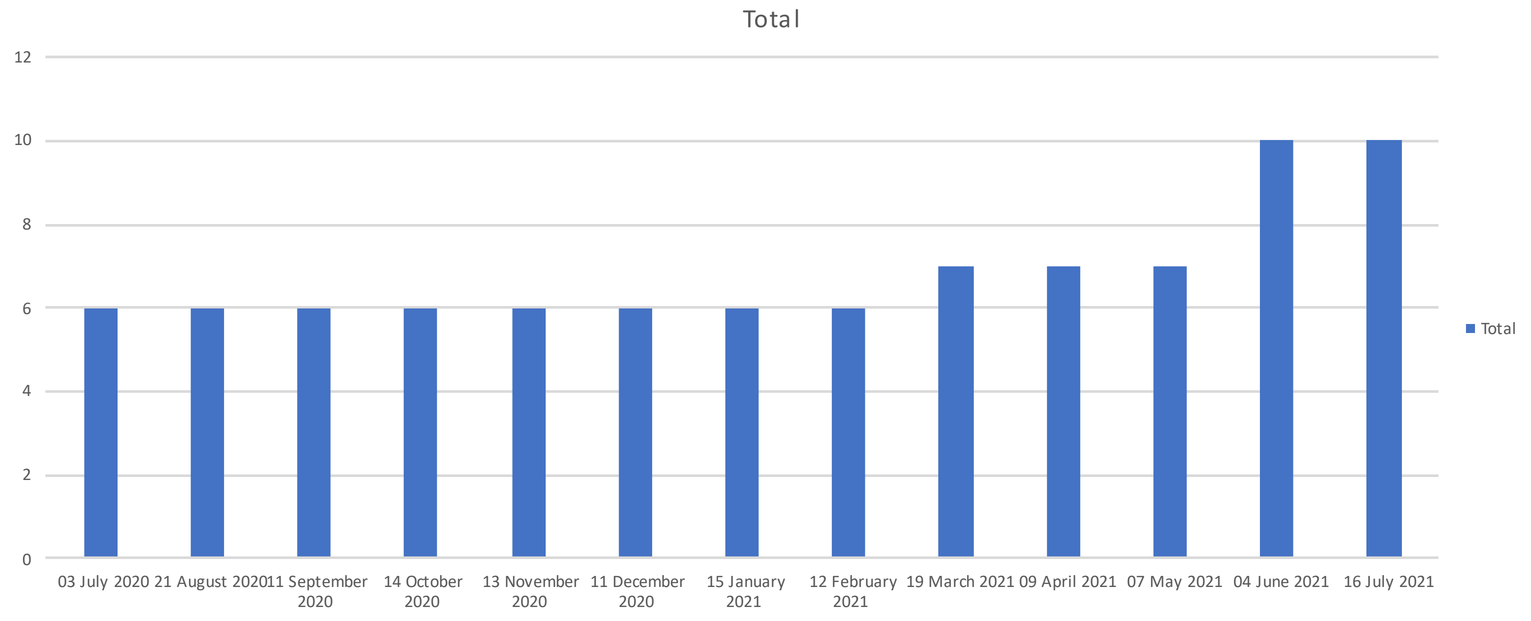
Sean Green
IT Director
E: sean.green@cityoflondon.gov.uk
T: 07715 234 487

Appendences

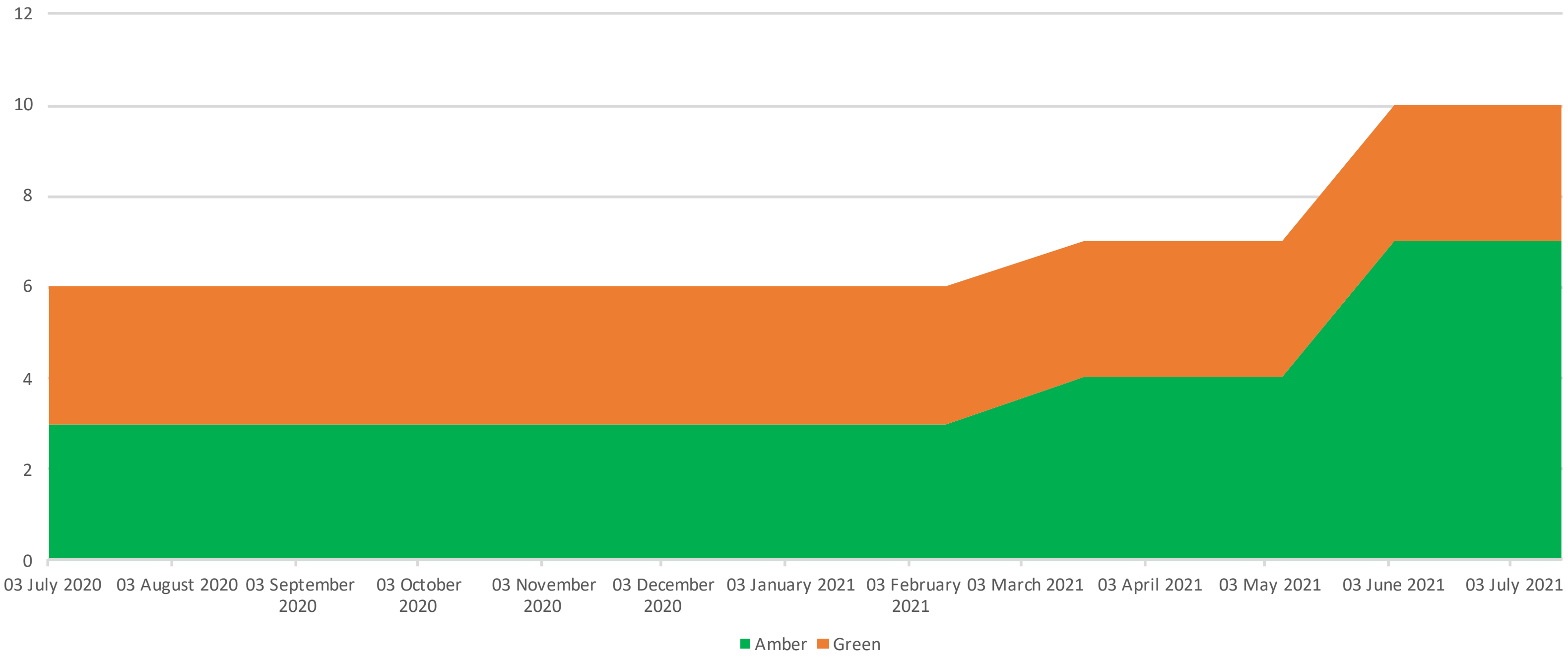
Appendix A – IT Risks Analysis
Appendix B- IT Corporate and Departmental Risks

Appendix A – IT Risks Analysis

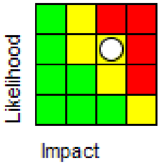
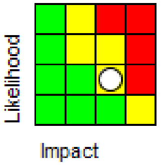
No of IT risks since July 2021

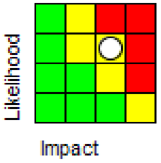
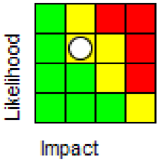


Amber /Green Risks July 2020 to July 2021



APPENDIX B - 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 Caroline Al-Beyerty	**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**	All Staff Mandatory Security training has been completed between April to June 2021 - any noncompliance will be reported A special one-off IT Cyber check paid for by LGA has been completed with remediation actions underway. New PSN Health check commissioned to commence, work started on this 28th June, results will be shared and actions to ensure compliance will be followed through once the report is received **11th August 2021**		**8**	30-Sep-2021 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 John Barradell	**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 • 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		**12**	New business intelligence dashboards continue to be developed for improved decision making by the Corporate Strategy and Performance team • An updated An Information Management Asset register has been populated for the organisation. Plan being developed for moving unstructured data from Shared Drives to SharePoint is being developed **11th August 2021**		**6**	31-Dec-2021 Reduce	▬ Constant