Committee(s)	Dated:
Audit and Risk Management Committee	26/02/2024
Subject: Corporate Risk – Deep Dive Reviews: CR16 Information Security; CR33 Major Capital Schemes	**Public**
Which outcomes in the City Corporation's Corporate Plan does this proposal aim to impact directly?	**N/A**
Does this proposal require extra revenue and/or capital spending?	**N**
If so, how much?	**N/A**
What is the source of Funding?	**N/A**
Has this Funding Source been agreed with the Chamberlain's Department?	**N/A**
Report of: the Chamberlain	**For Discussion**
Report author: Matt Lock, Head of Internal Audit	

Summary

Internal Audit has undertaken deep dive reviews in relation to CR16 Information Security and CR33 Major Capital Schemes. The objective of the deep dive reviews is to examine the effectiveness of the arrangements in place for the systematic management of Corporate Risk.

The review found that:

- For CR16, the risk is being reviewed regularly on system and updated accordingly although this has not identified that the implementation dates of 5 of the 6 stated mitigating actions are now in the past.
- The impact of the mitigating actions for CR16 have not been quantified and so it was not possible to assess the extent to which these will contribute to reduced risk.
- CR33 has not been reviewed and updated on a regular or sufficiently frequent basis.
- No mitigating actions have been recorded for CR33 and the overall target date for achieving the reduced target risk score is 9 months in the past.

The responsible officers engaged fully with this process, resulting in a transparent and full exchange of information, the findings of the deep dive review have been shared and it is anticipated that this will inform subsequent management review accordingly.

Recommendation(s)

Members are asked to note the report.

Main Report

Background

1. Deep-dive reviews of the City of London Corporation's Corporate Risks are undertaken by Internal Audit and reported to this Committee. The report is informed by in depth

review of the arrangements in place for managing risk, incorporating a quantitative assessment of the systematic application of the Corporate Risk Management Framework and a qualitative assessment as to the overall quality and completeness of the information provided in the risk register and, where possible, an objective review of the effectiveness of mitigating actions.

Current Position

2. The deep dive report takes the following format:

    i. Review of Risk Register Maintenance
    ii. Review of Completed Mitigating Actions
    iii. Review of Proposed Mitigating Actions
    iv. Review of Monitoring Arrangements
    v. General Observations and Overall Commentary

3. This report is focussed on Corporate Risks CR16 Information Security and CR33 Major Capital Schemes. The relevant extracts from the Risk Register are shown as Appendix 1 and 2 respectively.

CR16 Information Security

Area of Testing	Audit Findings
Risk Register Maintenance	▪ All key information fields are populated. ▪ The risk register has been reviewed on system 12 times in 12 months, which meets the requirements of the Risk Management Framework and is considered sufficiently frequent to ensure that Chief Officers are presented with timely information.
Mitigating Actions	▪ It is unclear to what extent mitigation actions will deliver positive outcomes and what impact these will have on the overall risk level. ▪ 5 out of 6 mitigating actions are overdue against stated timescales
Monitoring Arrangements	The risk has been reviewed monthly. From January 2024, Chief Officer responsibility for IT and, therefore, this risk, has transferred to the Chamberlain – the risk will be reviewed monthly by the Chamberlain's Senior Leadership Team in addition to the operational review undertaken by the IT Leadership Team.
General Observations and Overall Commentary	Based on the information in the Corporate Risk Register, Internal Audit cannot provide assurance that the target risk score will be reached by the specified target date of 31 March 2024. Updates against individual actions include statements which do not facilitate independent review of incremental progress in mitigating the overall risk; in some cases it is unclear what specific action (and impact) was expected by the individual due dates (now passed) and whether or not delivery against these was on track.

CR33 Major Capital Schemes

Area of Testing	Audit Findings
Risk Register Maintenance	▪ The basic information fields are populated and the risk is articulated, the mitigating action section, however, has not been populated. ▪ The risk has been reviewed infrequently, only 3 reviews in 2023 with the most recent being 5th September 2023. ▪ This does not meet the requirements of the Risk Management Framework and is not considered sufficiently frequent to ensure that Chief Officers are presented with timely information.
Mitigating Actions	▪ There are no mitigating actions identified for this risk ▪ The target date for achieving the overall reduced target risk score is some 9 months in the past.
Monitoring Arrangements	From January 2024, Chief Officer responsibility for Major Programmes and, therefore, this risk, has transferred to the Chamberlain – the risk will be reviewed monthly by the Chamberlain's Senior Leadership Team going forwards.
General Observations and Overall Commentary	On the basis of the limited information contained within the Corporate Risk Register and clarifications obtained from relevant officers, Internal Audit cannot provide assurance that the Corporate risk is being managed effectively through the Corporate Risk Management framework. The risk register does not reflect any planned mitigation activities within the 'action plan' section and it is unclear what action must be taken to achieve the target risk score; this is compounded by the target due date having been exceeded by over 9 months.

Corporate & Strategic Implications

4. Corporate Risks are those that threaten the City of London Corporation's ability to achieve its strategic objectives and top priorities. The Risk Management process is designed to identify and manage risk to the organisation and incorporates various assurance mechanisms, this deep dive process is one source of assurance, examining the extent to which Corporate Risks are being managed within the Corporate Risk Management framework.

Conclusion

5. Internal Audit has identified opportunities to improve the application of a systematic approach to managing risk and the extent to which the Corporate Risk Management framework is applied.

Appendices

- **Appendix 1:** Risk Register Extract – CR16
- **Appendix 2:** Risk Register Extract – CR33

Matt Lock
Head of Internal Audit
E: matt.lock@cityoflondon.gov.uk T: 020 7332 1276