| **Committee(s)** | **Dated:** |
|---|---|
| Audit and Risk Management Committee | 27/09/2022 |
| **Subject: Corporate Risk – Deep Dive Review: CR29 Information Management** | **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: Head of Internal Audit** | **For Discussion** |
| **Report author: Matt Lock** | |

## Summary

Internal Audit has undertaken a deep dive review in relation to CR29 Information Security. The objective of the deep dive review is to review the effectiveness of the arrangements in place for the systematic management of Corporate Risk.

The review found that:

- While risk register updates are completed frequently, as is required in practice for Corporate Risks and ensuring currency of information, there are no planned mitigating actions to manage this risk.
- Oversight and control of this risk is, in practice, split between two departments, which is not considered entirely effective.

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 and provide feedback on the extent to which they are satisfied the risk is being appropriately managed.

## 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 reports prepared are 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 Risk CR29 Information Security, the latest Risk Register extracts are shown as Appendix 1.

## CR29 Information Management

| Area of Testing | Audit Findings |
|---|---|
| Risk Register Maintenance | ▪ All key information fields are populated and have been updated when each review takes place, target dates for completion of mitigating actions are documented.<br>▪ The risk register has been updated monthly which meets the requirements of the Risk Management Framework and is considered sufficiently frequent to ensure that Chief Officers are presented with timely information. |
| Completed Mitigating Actions | ▪ A number of mitigating actions are noted as complete, Audit testing verified this to be accurate.<br>▪ While actions have been completed, there is no measure of their effectiveness and completion has resulted in no positive impact on the assessed overall level of risk; there is no reduction in likelihood or impact scoring. |
| Proposed Mitigating Actions | There are currently two stated mitigating actions:<br>▪ Implementation of outstanding Internal Audit Recommendations – Internal Audit follow-up work and subsequent discussion with management has verified that the outstanding Audit recommendations referred to will not be implemented, owing to resourcing constraints. The action, therefore, will not be completed.<br>▪ Development of an Information Management Maturity Plan – This action was formulated by the former IT Director, with other colleagues having insufficient knowledge to continue work in relation to this. It does not appear that this had been progressed and there is no knowledge of the benefits this might bring, it has been suggested that the Information Management Board will likely abandon this action. |

| | |
|---|---|
| | There are no further mitigations planned to reduce or manage this risk. |
| Monitoring Arrangements | While there is regular review and update of the risk register, this does not appear to have resulted in effective oversight, the risk is not being actively managed. There is a lack of clear ownership for managing this risk with a shared responsibility between IT and Comptroller's colleagues. |
| General Observations and Overall Commentary | The risk is being reviewed on a regular and timely basis, although there are no live actions or plans to mitigate this risk further. The Head of Internal Audit has recommended to Chief Officers Risk Management Group that consideration be given to whether the absence of resources to mitigate and manage this risk increases the current level of risk or whether the assessment of risk is incorrect (i.e. overstated and so does not warrant further action). |

**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. In the case of CR29, the deep dive review process has identified scope for more in-depth management of this risk, the regular review and update of the risk register had not identified that the planned mitigating actions were no longer valid. There are no planned actions to reduce or manage this risk.

**Appendices**

- **Appendix 1:** Risk Register Extract - CR29 Information Management

**Matt Lock**
Head of Internal Audit, Chamberlain's Department

E: matt.lock@cityoflondon.gov.uk
T: 020 7332 1276