



CROYDON

Final Internal Audit Report

Risk Management

October 2019

Distribution: Executive Director of Resources and Monitoring Officer (Final only)
Director of Finance Investment and Risk and S151 Officer
Head of Risk and Corporate Programme Office
Risk and Corporate Programme Officer

Assurance Level	Issues Identified	
Substantial Assurance	Priority 1	0
	Priority 2	2
	Priority 3	2

Confidentiality and Disclosure Clause

This report ("Report") was prepared by Mazars LLP at the request of London Borough of Croydon and terms for the preparation and scope of the Report have been agreed with them. The matters raised in this Report are only those which came to our attention during our internal audit work. Whilst every care has been taken to ensure that the information provided in this Report is as accurate as possible, Internal Audit have only been able to base findings on the information and documentation provided and consequently no complete guarantee can be given that this Report is necessarily a comprehensive statement of all the weaknesses that exist, or of all the improvements that may be required.

The Report was prepared solely for the use and benefit of London Borough of Croydon and to the fullest extent permitted by law Mazars LLP accepts no responsibility and disclaims all liability to any third party who purports to use or rely for any reason whatsoever on the Report, its contents, conclusions, any extract, re-interpretation, amendment and/or modification. Accordingly, any reliance placed on the Report, its contents, conclusions, any extract, re-interpretation, amendment and/or modification by any third party is entirely at their own risk.

Please refer to the Statement of Responsibility in Appendix 3 of this report for further information about responsibilities, limitations and confidentiality.

Executive Summary

1. Introduction.....	3
2. Key Issues.....	3

Detailed Report

3. Actions and Key Findings/Rationale	5
4. Priority Three Issues.....	7

Appendices

1. Terms of Reference
2. Definitions for Audit Opinions and Identified Issues
3. Statement of Responsibility

1. Introduction

- 1.1 The Risk and Corporate Programme Office (RCPO) has a fundamental role in evaluating and reforming the Risk Management framework, which has been contextualised within the Practical Guide to Risk Management. Aside from being the embodiment of the framework, the guide acts as resource geared towards promoting the importance and understanding of risk.
- 1.2 To further promote the framework, the RCPO has established training sessions that are held periodically, and the role of 'Risk Champion' who is responsible for encouraging a risk aware culture particularly at a strategic level through their involvement in ensuring risk management objectives are achieved.
- 1.3 The RCPO has direct involvement in each of the five stages of Risk Management, from being an aid in the identification, management and monitoring of risks at quarterly DMT meetings, to reporting high impact risks to the Governance Board, the Executive Leadership Team and the General Purposes & Audit Committee.
- 1.4 All staff and functions have a role and therefore responsibility in the operation of the Risk Management process. These roles are highlighted in the Practical Guide to Risk Management.
- 1.5 The objectives, methodology and scope are contained in the Audit Terms of Reference at Appendix 1.

2. Key Issues

Priority 2 Issues

The Risk and Corporate Programme Office (RCPO) attends departmental management team (DMT) meetings to review the departmental / divisional risk registers and obtain updates, which are then used to update the risk entries on the JCAD risk management system; however:

- attendance at these DMT meetings is only quarterly and more frequent updates, where appropriate, are not always volunteered;
- the RCPO is reliant on the DMT to agree the wording of any changes to the risk entry recorded on JCAD, which in some instances can take time and several iterations; and
- some DMT's are not fully engaging and are either cancelling or postponing their quarterly reviews or not responding to meeting requests. **(Issue 1.)**

Sample testing identified that because the controls detailed in JCAD risk management system were not sufficiently detailed it was difficult to:

- determine in all instances how the controls helped or would help mitigate the risks; and
- establish the target timescales and progress being made in the implementation of future controls. **(Issue 2.)**

The Priority 3 issues are included under item 4.

3. Actions and Key Findings/Rationale

<u>Control Area 4: Management of Risks</u>		
Priority	Action Proposed by Management	Detailed Finding/Rationale – Issue 1
2	<p>The Risk & CPO Team recognise that there are challenges with accountable officers / risk owners satisfactorily amending and updating their risk entries following identification of the need and agreement to complete actions during the DMT / DLT meetings.</p> <p>The Risk Management Team will review the 'Practical Guide to Risk Management' to ensure instruction is clear to all officers and also to reflect current practice.</p> <p>The Risk & CPO Team are limited as a resource (1 officer 0.5 fte assigned to risk and 1 Head of Service who also has 3 other services to manage) and therefore strategically apply the majority of the available resource focus to ensuring each of the 20 DMT and 5 DLT meetings are attended by the risk officer each quarter.</p> <p>The Risk & CPO Team will endeavour to request support from the Council's</p>	<p>The Council's Risk Management Policy Statement & Strategy details that, 'All staff will be given appropriate training and guidance to enable them to take responsibility for managing risk within their own working environment. All named risk owners have access to the corporate wide risk register system and will be required to update and maintain their entries on the system.' The Council's 'Practical Guide to Risk Management' further details that, 'Departments should review their risks at least once on a monthly basis for high rated risks and on a 3 monthly basis for all other risks.'</p> <p>Croydon Council uses the JCAD risk management system to record details and ownership of identified corporate risks and their associate control measures. The Risk & Corporate Programme Office Team manages the delivery of the Council's Risk Management Framework and the management and administration of the database.</p> <p>It was established that the Risk & Corporate Programme Office (RCPO) attends departmental management team (DMT) meetings on a quarterly basis to review the departmental / directorate risk registers and that any updates provided at these meetings are then used by the RCPO to update the risk entry on the JCAD risk management system; however, there are some issues with this process, as follows:</p> <ul style="list-style-type: none"> • Attendance at the DMT meetings is only quarterly and more frequent updates, where appropriate, are not always volunteered. • The RCPO is reliant on the DMT to agree the wording of any changes to the risk entry recorded on JCAD, which in some instances can take time and several iterations.

	<p>Executive Leadership Team that will strongly encourage full co-operation from all risk owners and clarity that the corporate risk management framework is acknowledged and complied with in respect of ensuring quarterly risk reviews are always completed.</p>	<ul style="list-style-type: none"> Some DMT's are not fully engaging and are either cancelling or postponing their quarterly reviews or not responding to meeting requests. <p>There is a risk that departments are not taking full ownership and not complying with the Council's published Risk Management Framework fully. This results in the Council's corporate risk register not being fully up to date and, therefore, a less effective tool.</p>
<p>Responsible officer</p>	<p>Deadline</p>	
<p>Head of Risk & CPO</p>	<p>Immediate</p>	

<u>Control Area 5: Risk Monitoring and Reporting</u>						
Priority	Action Proposed by Management	Detailed Finding/Rationale – Issue 2				
2	<p>The Risk & CPO Team has designed a bespoke report within the JCAD risk management system that will list in detail, all open ‘future controls’ with their ‘generated’ date stated.</p> <p>This will provide a clear focus for all concerned officers (Risk & CPO, risk owners and leadership teams) to quantify the future control risk statement and ensure clarity in respect of detail and deadline(s) stipulated.</p>	<p>The Council’s ‘Practical Guide to Risk Management’ details that, ‘When reviewing risks check that control measures are being actioned so they can make a real difference to the likelihood or impact of a risk – regularly monitor and update control measures.’</p> <p>Examination of the control measures linked to a sample of 20 different risks within JCAD identified that, although the controls had a heading (‘Control Measure’), which provided a basic summary of the existing and future controls, none of the ‘control details’ were completed. Thus it was difficult to:</p> <ul style="list-style-type: none"> • determine in all instances how the controls helped or would help mitigate the risks; and • establish the target timescales and progress being made in the implementation of future controls. 				
	<table border="1"> <thead> <tr> <th>Responsible officer</th> <th>Deadline</th> </tr> </thead> <tbody> <tr> <td>Risk & CPO Officer</td> <td>Ongoing</td> </tr> </tbody> </table>	Responsible officer	Deadline	Risk & CPO Officer	Ongoing	<p>Where controls, and in particular future controls, are not sufficiently detailed, there is a risk that the implementation of these may not be easily monitored or that these may not be appropriately prioritised.</p>
Responsible officer	Deadline					
Risk & CPO Officer	Ongoing					

4. Priority 3 Issues

Action Proposed by Management	Findings
<p>1) A benchmarking document has been developed by the Risk & CPO Team and will be distributed to the members of the Insurance London Consortium (ILC) for completion and analysis. LB Croydon will be the lead borough and will use the information to identify any practices, policies or procedures that could enhance the service delivery for LB Croydon.</p>	<p>Benchmarking is a useful tool to provide assurance on the risk register and helps identify emerging and new risks.</p> <p>It was established that the Corporate Programme Office had recently ended their engagement with CIPFA for benchmarking reports. Discussions established that this was due to a limited number of authorities contributing to the benchmarking (for the latest 2017 benchmarking it was only Barnsley; Cleveland Fire Authority; Cornwall; Croydon; Jersey; Oxford; Shropshire; St. Helens; Stoke-on-Trent and Tower Hamlets) and the benchmarking being based on a self-assessment questionnaire being completed by each local authority, which could be less objective.</p> <p>The RCPO explained that it was instead planned to conduct a benchmarking exercise against the members of the Insurance London Consortium, which would increase the relevance of the benchmarking data as all constituents would be London based authorities. The new questionnaire will be comprised of 20 questions, requiring a comprehensive answer for each.</p> <p>Where benchmarking is not conducted, it is more difficult to obtain assurance on the robustness of the risk register and there is a risk that new and emerging risks may be missed or not identified in a timely manner.</p>
<p>2) The Risk & CPO Team acknowledge that the reference to 'risk champions' and their role as detailed in The Practical Guide to Risk Management is now obsolete. The Practical Guide to Risk Management will be reviewed and amended to reflect the current Risk Management Framework delivery practice.</p>	<p>The Practical Guide to Risk Management details that the role of Risk Champions is '<i>to champion the cause of risk management within each department, particularly at the strategic level; to take personal responsibility for ensuring that the risk management objectives set out in the policy are achieved and to encourage a risk aware culture in all areas of the organisation</i>'.</p> <p>Discussion with the Risk & Corporate Programme Officer established that Risk Champions had not been formally appointed, rather it was assumed that directors/risk owners were aware that their role is to promote an appropriate risk management culture and champion risk, i.e. the role of a Risk Champion and Risk Owner was the</p>

	<p>same. Based on examination of the Practical Guide to Risk Management, it is not clear that these roles are interchangeable.</p> <p>Examination of the Executive Directors' Assurance Statement template identified that there is no mention of 'Risk Champions'.</p> <p>Where risk champions have not been established and been made aware of their responsibilities, there is a risk that they do not have a fundamental role in promoting risk in the Council as the guidance suggests. This could result in officers not recognising the importance of risk management and areas of exposure not being acknowledged and reported.</p>
--	---

TERMS OF REFERENCE

Risk Management

1. INTRODUCTION AND BACKGROUND

- 1.1 The following four stages encompass the Council's risk management strategic objective:
 - Identify corporate and operational risks
 - Assess the risks for likelihood and impact
 - Identify mitigating controls
 - Allocate responsibility for the mitigating controls
- 1.2 It is the responsibility of Directors and Heads of Service to identify the exposure to risk within their division.
- 1.3 Each identified risk is reported to the Risk and Corporate Programme Office Officer at a departmental management team (DMT) meeting that is held quarterly with each department of the Council. During the DMT, the Risk and Corporate Programme Officer will update the risk register on the JCAD system to reflect the new risks that have been identified, or to update pre-existing risks.
- 1.4 Each risk is assigned a risk owner whom is responsible for ensuring that actions are taken to mitigate exposure. It is the responsibility of the risk owner to send a follow up on the progress of the actions that are/have been undertaken. Progress updating is done on an ad hoc basis, in some cases taking the form of a follow up meeting with Risk and Corporate Programme Office Officer.
- 1.5 A Risk Management Steering Group meets to develop a formal risk management framework with a view to 'achieve the Council's strategic policies and the delivery of services to the community.' The Steering Group consists of 'Risk Champions' from every department, a representative from Internal Audit, the Head of Risk Management & Insurance, and the Risk & Corporate Programme Team.
- 1.6 The General Purposes and Audit Committee (GPAC) meet on a quarterly basis to provide oversight on the risk management framework, as well as to discuss 'Red Risks'.
- 1.7 This audit is being undertaken as part of the agreed Internal Audit Plan for 2019/20.

2. OBJECTIVES AND METHODOLOGY

- 2.1 The overall audit objective is to provide an objective independent opinion on the adequacy and effectiveness of the control environment relating to Risk Management.
- 2.2 In order to achieve the overall objectives, a risk based systems audit approach will be carried out, documenting and evaluating the actual controls against those expected and based on this, undertaking appropriate testing conducted.

- 2.3 The key findings, conclusions, and subsequent issues arising will be presented at an exit meeting and followed by the circulation of a draft report for consideration by management. This prior to agreement and issue of the final audit report.

3. SCOPE

This audit examined the Council's arrangements in relation to Risk Management, and include the following areas:

Control Areas/Risks	Issues Identified		
	Priority 1 (High)	Priority 2 (Medium)	Priority 3 (Low)
Legislative, Operational, and Management Requirements	0	0	0
Risk Identification	0	0	0
Assessment of Risks	0	0	0
Management of Risks	0	1	1
Risk Monitoring and Reporting	0	1	1
TOTAL	0	2	2

DEFINITIONS FOR AUDIT OPINIONS AND IDENTIFIED ISSUES

In order to assist management in using our reports:

We categorise our **audit assurance opinion** according to our overall assessment of the risk management system, effectiveness of the controls in place and the level of compliance with these controls and the action being taken to remedy significant findings or weaknesses.

	Full Assurance	There is a sound system of control designed to achieve the system objectives and the controls are consistently applied.
	Substantial Assurance	While there is basically a sound system of control to achieve the system objectives, there are weaknesses in the design or level of non-compliance which may put this achievement at risk.
	Limited Assurance	There are significant weaknesses in key areas of system controls and/or non-compliance that puts achieving the system objectives at risk.
	No Assurance	Controls are non-existent or weak and/or there are high levels of non-compliance, leaving the system open to the high risk of error or abuse which could result in financial loss and/or reputational damage.

Priorities assigned to identified issues are based on the following criteria:

Priority 1 (High)	Fundamental control weaknesses that require the immediate attention of management to mitigate significant exposure to risk.
Priority 2 (Medium)	Control weakness that represent an exposure to risk and require timely action.
Priority 3 (Low)	Although control weaknesses are considered to be relatively minor and low risk, action to address still provides an opportunity for improvement. May also apply to areas considered to be of best practice.

STATEMENT OF RESPONSIBILITY

We take responsibility to the London Borough of Croydon for this report which is prepared on the basis of the limitations set out below.

The responsibility for designing and maintaining a sound system of internal control and the prevention and detection of fraud and other irregularities rests with management, with internal audit providing a service to management to enable them to achieve this objective. Specifically, we assess the adequacy and effectiveness of the system of internal control arrangements implemented by management and perform sample testing on those controls in the period under review with a view to providing an opinion on the extent to which risks in this area are managed.

We plan our work in order to ensure that we have a reasonable expectation of detecting significant control weaknesses. However, our procedures alone should not be relied upon to identify all strengths and weaknesses in internal controls, nor relied upon to identify any circumstances of fraud or irregularity. Even sound systems of internal control can only provide reasonable and not absolute assurance and may not be proof against collusive fraud.

The matters raised in this report are only those which came to our attention during the course of our work and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. Recommendations for improvements should be assessed by you for their full impact before they are implemented. The performance of our work is not and should not be taken as a substitute for management's responsibilities for the application of sound management practices.

This report is confidential and must not be disclosed to any third party or reproduced in whole or in part without our prior written consent. To the fullest extent permitted by law Mazars LLP accepts no responsibility and disclaims all liability to any third party who purports to use or rely for any reason whatsoever on the Report, its contents, conclusions, any extract, reinterpretation amendment and/or modification by any third party is entirely at their own risk.

Registered office: Tower Bridge House, St Katharine's Way, London E1W 1DD, United Kingdom.
Registered in England and Wales No 0C308299.