CITY OF LONDON

CHAMBERLAIN'S DEPARTMENT

INTERNAL AUDIT SECTION

LONDON COUNCILS

Risk Management and Business Continuity Planning (2015-16)

FINAL REPORT

Date Issued: May 2016

Issued to: Christiane Jenkins, Director of Corporate Governance
Frank Smith, Director of Corporate Resources
David Sanni, Head of Financial Accounting

CONTENTS (INDEX)

Audit Fieldwork completed	17 March 2016
Draft Report Issued	22 March 2016
Management Response Received Agreeing Recommendations	11 April 2016
Final Report Issued	13 May 2016

SECTION A: EXECUTIVE SUMMARY

Introduction

This review was undertaken as part of the agreed internal audit plan for 2015-16.

London Councils is a cross-party organisation, funded by London member authorities comprising of 32 London boroughs and the City of London.

At the time of the audit the Draft Business Continuity Plan (BCP) had been reviewed by Corporate Management Board (CMB) and was due to be finalised in March 2016.

The Risk Management Strategy & Framework was last updated and approved in May 2012.

Assurance Level	Description
Moderate Assurance 'Amber'	An adequate control framework is in place but there are weaknesses and/or a lack of compliance which may put some system objectives at risk.

Recommendations	Red	Amber	Green	Total
Number Made:	0	1	2	3
Number Accepted:	0	1	2	3

SECTION B – AUDIT FINDINGS

Key Findings:

Risk Management Strategy & Framework

London Councils has developed a formal risk management process for the management of intrinsic, long term and service delivery risks, providing assurance that the organisation is able to function effectively and achieve its aims.

The Risk Management Strategy & Framework contains the following information:

- Identifying risks
- Assessing and scoring risks
- Risk Scores
- Mitigating Risks
- Reviewing the Risk Register
- Roles and Responsibilities

The Risk Management Strategy & Framework was last reviewed and updated, as presented to the London Councils' Audit Committee in 2012. In the absence of regular review of the Risk Management Strategy & Framework, it may not be reflective of current organisational processes and in alignment with the Business Plan 2015-16. **(Recommendation 1)**

Links between Business Plan, Risk Registers and Business Continuity Plan

London Councils' Business Plan 2015-16 sets out the five broad, over-arching themes for the year. It describes the ways in which London Councils goes about its operations with members, member authorities and others.

The directorate programmes detail the range of operations and work that will support the overall objectives, all of which relate in some way to the over-arching themes of resourcing London, securing devolution and localism, supporting London and organisational change.

On review of the risk registers and the Business Continuity Plan (BCP) we noted that they are clearly linked to the Business Plan and escalation processes are in place to ensure that organisational change is reflected in the BCP and risk registers.

Assurance that controls are operating effectively

Each Directorate or division is required to maintain a risk register relating to their work. We selected two risks from the Services risk register to ensure that assurance is provided

that controls in place are operating effectively. The risks selected were as follows:

A5 - Breaches in data protection and security that leads to the mishandling or misplacing of commercial, sensitive and/or personal data
B3 - Taxicard applications for in-house processing not assessed on time.

During discussions with the Chief Contracts Officer and Head of Community Services and Grants, we verified that assurances have been identified and can be evidenced to show that controls are operating effectively.

The following documentation was reviewed to evidence the controls in place:

- Act Now – Data Protection and Risk Management Training
- Data Protection and Security Agreement
- London Councils Grant Scheme 2013-15 Project Handbook
- London Councils Grants Team Manual
- Taxicard Key Performance Indicators

Reporting of Risk Management

London Councils' Risk Management Strategy & Framework states that the Corporate Risk Register will be presented to the Audit Committee on an annual basis. We verified that the Audit Committee had been presented with an annual report from the Director, Corporate Governance on risk management, which includes the current versions of the directorate and Corporate Risk Registers.

In September 2011 the Audit Committee requested that the directorate risk registers were presented to the committee in rotation, one at each meeting. We obtained the following directorate risk registers and verified that they had been presented to the Audit Committee:

- Chief Executive – March 15
- Services – June 15
- CRR – September 15

The Directorate, Divisional and Corporate Risk Registers are reviewed half-yearly by London Councils' Corporate Management Board (CMB), as set out in the agreed Risk Management Strategy & Framework. This review process ensures that the risk registers continue to reflect London Councils' corporate priorities and can be updated to take account of any threats or opportunities.

We obtained the last two risk register update reports that were presented to CMB in February 2016 and August 2015.

We noted that the Risk Register update reports include information on the following:

- Current position
- Presentation to Audit Committee
- Corporate Risk Register
- Chief Executive's Directorate Risk Registers
- Policy and Public Affairs Directorate Risk Register
- Services Directorate Risk Register
- Implications

Business Continuity Plan Roles and Responsibilities

A draft BCP has been produced (January 2016) to provide managers and staff with up to date information and step-by-step guidance on how best to respond to a range of disruptive situations that would, if not addressed, lead to the failure of the service.

The plan contains details of Directorate key functions, staff, resources and essential contact numbers for use in a situation likely to disrupt business. The Plan is intended as a guide to provide a basis for informed decision-making in dealing with a range of abnormal situations.

The draft BCP contains the following information:

- Plan Management
- Critical Function Priority List
- Roles and responsibilities
- Business Impact Analysis
- Types of business continuity incidents and recommended actions
- Resource and access to service
- Plan supplements
- Third party arrangements

Roles and responsibilities are detailed within the BCP. Roles and responsibilities have been designated to teams:

- Gold
- Silver
- Bronze

Each team has its own roles and responsibilities to ensure that the BCP is effective in the event of a disaster. Team members have been stated within the BCP along with their contact details and role/responsibility.

Reporting of the Business Continuity Plan

The BCP does not contain a reporting mechanism for the BCP test results to the Audit Committee. In the absence of a full disaster recovery report of results, the Audit Committee does not have assurance that the Business Continuity processes in place are sufficient to protect London Councils from potential disruption. **(Recommendation 2)**

Testing of the Business Continuity Plan

A testing timetable forms part of the BCP. On review of the timetable we noted that only certain aspects of the BCP have been scheduled for testing e.g. Remote Access Service capacity testing (post 2FA upgrade). The types of potential business continuity incidents listed had not yet been included for testing. In the absence of full BCP testing, London Councils do not have assurance that business continuity arrangements in place are effective at continuing business operations in the event of an incident. **(Recommendation 3)**

Business Impact Assessments and Content of the Draft BCP

The Silver and Bronze teams have identified their own key tasks where necessary in order of priority by completing the Service Impact Analysis. This is used to determine urgent and non-urgent tasks within their service area. On review of the Business Impact Assessments we noted that 10 business impact assessments had not yet been completed. The ICT & Facilities Manager provided a timetable of when the business impact assessments will be completed.

However we noted that at present the BCP does not state how often the business impact assessments will be reviewed and updated by directorates. In the absence of regular review, London Councils may be at risk of not updating the BCP to reflect organisational change which impacts the effectiveness of the BCP.

Additionally on review of the draft BCP we noted that the following information is not stated:

- Review and approval process of the Business Continuity Plan
- Scenario testing timetable
- Reporting results of scenario testing
- Business Impact Analysis review and update timetable
- Roles and responsibilities of City of London, Agilisys and London Councils
- Critical systems and associated Recovery Time Objective (RT0)
- Relevant stakeholders

(Recommendation 3)

Risk Management Strategy & Framework

Priority	Issue	Risk
Green	The Risk Management Strategy & Framework was last formally reviewed and approved by the Audit Committee in May 2012.	The Risk Management Strategy & Framework is not reflective of current organisational processes. Risk Management Strategy & Framework not in alignment with the Business Plan 2015-16.

Recommendation 1:

The Risk Management Strategy & Framework should be scheduled for review and update every three years to ensure that it is reflective of current organisational processes and subsequently approved by the Audit Committee.

Management Response and Action Plan

Management is happy for a recommendation to be made to the Audit Committee when this Internal Audit Report is reported, that the Risk Management Strategy & Framework is formally reviewed during the course of 2016/17 and any proposed changes are reported to Audit Committee for approval and that it is then reviewed on a periodic basis.

Responsibility: Christiane Jenkins, Director, Corporate Governance
Target Implementation Date: September 2016

* Where recommendation not accepted indicate alternative action that will be taken to mitigate risk or reasoning for accepting risk exposure to be provided

Reporting of the Business Continuity Plan

Priority	Issue	Risk
Green	Test results of the Business Continuity Plan are not scheduled to be presented to Audit Committee.	Business Continuity processes in place are insufficient to protect London Councils from potential disruption.

Recommendation 2:

When the Business Continuity Plan is tested, the results should be recorded and presented to Audit Committee. This requirement should be updated in the Business Continuity Plan.

Management Response and Action Plan

The results of the Business Continuity Plan (BCP) tests will be recorded and reported to

the Audit Committee. The BCP will be updated to reflect this.

Responsibility: Roy Stanley, Information & communications technology and facilities manager
Target Implementation Date: Completed

* Where recommendation not accepted indicate alternative action that will be taken to mitigate risk or reasoning for accepting risk exposure to be provided

Business Impact Assessments and Content of the Draft BCP

Priority	Issue	Risk
Amber	The draft Business Continuity Plan does not contain information to enable effective business continuity arrangements to be undertaken	The Business Continuity Plan is not effective in the event of an incident.

Recommendation 3:

Prior to the finalisation of the Draft Business Continuity Plan the following should be considered for inclusion:

- Review and approval process of the Business Continuity Plan
- Scenario testing timetable
- Reporting results of scenario testing
- Business Impact Analysis review and update timetable
- Roles and responsibilities of City of London, Agilisys and London Councils
- Identification of critical systems and associated recovery time objective (RTO)
- Relevant stakeholders

Management Response and Action Plan

The recommendation is accepted and the listed items have been considered and incorporated as follows:

Review and approval process of the Business Continuity Plan – The plan is scheduled for review every three months by the ICT and Facilities Manager (the Core Plan Owner) and any relevant information such as structure charts and contact details updated. Any significant changes to the plan layouts will be referred to CMB for approval.

Scenario testing timetable – This timetable will be included within Appendix A which has been redrafted. It will be split into quarterly projected tasks over the next twelve months.

Reporting results of scenario testing – A third column will be added to Appendix A outlining the test results.

Business Impact Analysis (BIA) review and update timetable – This will be the

responsibility of each of the BIA plan owners and the overall responsibility of the Silver Team leads as outlined in Sections 2 and 4 of the plan.

Roles and responsibilities of City of London, Agilisys and London Councils – This level of detail will be outlined within the 'Critical Systems and Associated RTO' document, currently being drafted, which will hold the more technical details to the plan. Their roles and responsibilities are also outlined in section 4 of the current ICT Strategy 2015-18 documents.

Identification of critical systems and associated recovery time objective (RTO) – This level of detail will also be outlined within the 'Critical Systems and Associated RTO' document which will hold the more technical details to the plan.

Relevant stakeholders – This is detailed within the current ICT Strategy 2015-18 document."

Responsibility: Roy Stanley, Information & communications technology and facilities manager

Target Implementation Date: Completed

* Where recommendation not accepted indicate alternative action that will be taken to mitigate risk or reasoning for accepting risk exposure to be provided

APPENDIX 1: AUDIT DEFINITIONS AND RESPONSIBILITIES

Assurance levels

Category	Definition
Nil Assurance 'Dark Red'	There are fundamental weaknesses in the control environment which jeopardise the achievement of system objectives and could lead to significant risk of error, fraud, loss or reputational damage being suffered.
Limited Assurance 'Red'	There are a number of significant control weaknesses and/or a lack of compliance which could put the achievement of system objectives at risk and result in error, fraud, loss or reputational damage.
Moderate Assurance 'Amber'	An adequate control framework is in place but there are weaknesses and/or a lack of compliance which may put some system objectives at risk.
Substantial Assurance 'Green'	There is a sound control environment with risks to system objectives being reasonably managed. Any deficiencies identified are not cause for major concern.

Recommendation Categorisations

Priority	Definition	Timescale for taking action
Red - 1	A serious issue for the attention of senior management and reporting to the appropriate Committee Chairman. Action should be initiated immediately to manage risk to an acceptable level	Less than 1 month or more urgently as appropriate
Amber - 2	A key issue where management action is required to manage exposure to significant risks, action should be initiated quickly to mitigate the risk.	Less than 3 months
Green - 3	An issue where action is desirable and should help to strengthen the overall control environment and mitigate risk.	Less than 6 months

Note:- These 'overall assurance level' and 'recommendation risk ratings' will be based upon auditor judgement at the conclusion of auditor fieldwork. They can be adjusted downwards where clear additional audit evidence is provided by management of controls operating up until the point of issuing the draft report.

APPENDIX 2 – SCOPE AND EXCLUSIONS

SCOPE OF THE REVIEW

Internal Audit examined evidence that:

- A Risk Management Framework was in place and made available to all staff;
- Links were clearly seen between the London Councils' business plan, risks in the risk register and Draft Business Continuity Plan;
- Assurances have been identified and can be evidenced to show that controls are operating effectively;
- Risk management was regularly reported to Corporate Management Board and Audit Committee;
- The Draft Business Continuity plan clearly sets out roles and responsibilities and resources required to invoke such plans;
- The Draft Business continuity plan has been scheduled for regular testing. Testing has been undertaken prior to the implementation of the revised Business Continuity Plan;
- Reporting of the Business Continuity Plan once implemented to provide assurance that the Business Continuity was effective in continuing business operations;
- Business impact assessments have been undertaken to feed into the Business Continuity Plan;

EXCLUSIONS

- Our findings did not provide assurance that every risk on the risk register is being effectively controlled at an operational level
- We did not comment on the organisation's risk appetite definition but confirmed if it has been defined and clearly communicated
- We did not provide an opinion in relation to the risk strategies and policies
- We did not independently test the Business Continuity Plan
- Testing was focused on the Draft Business Continuity Plan
- This audit did not review or comment on the disaster recovery arrangements in place.
- Any testing undertaken as part of this audit was compliance based and sample testing only.

Our work does not provide any guarantee against material errors, loss or fraud or provide an absolute assurance that material error, loss or fraud does not exist.

What Happens Now?

Internal audit will carry out a follow-up exercise approximately six months after the issue of the final audit report. The ongoing progress in implementing each recommendation is reported by Internal Audit to each meeting of the Audit & Risk Management Committee.

Any Questions?

If you have any questions about the audit report or any aspect of the audit process please contact Pat Stothard, Head of Audit & Risk Management via email to pat.stothard@cityoflondon.gov.uk.