Final Internal Audit Report

Design of New Backup and Disaster Recovery Solution

June 2018

Distribution:

Executive Director Resources (Final only)

Head of ICT and Transformation

Information Manager

ICT Service & Contract Manager

Assurance Level	Recommendations Made	
Substantial Assurance	Priority 1	0
	Priority 2	2
	Priority 3	0

Contents

Page

Executive Summary

Detailed Report

Appendices

Executive Summary

1. Introduction

1.1 The Council's Backups and Disaster Recovery (DR) processes are currently managed by the Council's internal IT department together with its IT service provider (Capita). However, the Council is in the process of changing its DR solution to the proposed cloud based Microsoft Azure Site Recovery services. It was agreed that the focus of the audit will be on this new solution. The audit thus focused on the design of the new DR solution, in particular at expected backup and DR controls against the current design of the new solution.

1.2 This audit is part of the Internal Audit Plan for 2017/18. The audit objectives, methodology and scope are contained in the Audit Terms of Reference at Appendix 1.

2. Key Issues

No Priority 1 and 3 issues were raised.

Priority 2 issues are detailed under item 3. Please note, there are a number of expected controls that are currently not implemented because the Council is in the process of implementing the new backup and recovery processes. As a result, we have only reported issues where controls had not been considered in the implementation of the new solution. However, the Council will also need to ensure that those controls expected to be but not yet implemented are also actioned as a matter of priority during the project.

3. Actions and Key Findings/Rationale

<table>
<tr><td colspan="4"><u>Control Area 1: Disaster Recovery Procedures</u></td></tr>
<tr><td>Priority</td><td colspan="2">Action Proposed by Management</td><td>Detailed Finding/Rationale – Issue 1</td></tr>
<tr><td>2</td><td colspan="2">As we are moving to cloud for our Data Centre & DR services, there is less reliance on the council having a “Salvage & Relocation Procedure”, as this will be part of the cloud provider's procedures.

Having discussed this recommendation with our SDP Capita, we are both in agreement that at this stage implementing such a procedure for the council is not required.</td><td rowspan="3">In order that assets/resources, which are not fully effected by a disaster, are appropriately recovered and relocated, a “Salvage and Relocation Procedure” should be developed, with the procedure being included within the DR Plan.

Salvage and Relocation Procedures are not in place for the salvage and relocation of assets/resources, such as IT assets which may not be fully effected by the disaster.

Without proper salvage and relocation arrangements assets/resources which are not fully effected by the disaster may not be recovered and relocated.</td></tr>
<tr><td colspan="2">Responsible officer</td><td>Deadline</td></tr>
<tr><td colspan="2">Enterprise Architect</td><td>No further action</td></tr>
</table>

<table>
<tr><td colspan="3"><u>Control Area 8: Insurance Cover</u></td></tr>
<tr><td>Priority</td><td>Action Proposed by Management</td><td>Detailed Finding/Rationale – Issue 1</td></tr>
<tr><td>2</td><td>Having discussed this further with the Insurance team, they have recommended that we implement our new cloud DR solution and then look at what insurance if any we could take up.

We will request the CIO Director to discuss with Director of Finance about securing emergency funds within the annual budget for disaster recovery purposes.</td><td rowspan="3">In order to help minimise the impact of a disaster, appropriate insurances should be in place. Furthermore, emergency funds should be allocated within the annual budget for disaster recovery.

An insurance policy for disaster recovery for the Council could not be provided. Furthermore, evidence could not be provided to verify if emergency funds have been allocated for disaster recovery.

The lack of an insurance policy and an emergency fund for Disaster Recovery may result in delays in recovery of critical services due to the shortage of funds.</td></tr>
<tr><td>Responsible officer</td><td>Deadline</td></tr>
<tr><td>Enterprise Architect</td><td>31 July 2018</td></tr>
</table>

Appendix 1

GAP ANALYSIS

This audit was undertaken at a time when the Council was changing their backup and recovery processes and controls. As a result, the audit focused on comparing the solution intended to be implemented against the expected controls covered in an audit of this area. Detailed below is our comparison of the expected controls, controls already implemented, controls to be implemented and controls that have not been considered by the Council.

Expected Control	Control as Implemented	Control Expected but not yet Implemented	Control not Expected/outstanding
Disaster Recovery Strategy or a Disaster Recovery Plan (DR Plan) has been documented and approved.	The legacy DR Plan/Capita IT DR Plan is in place. However, the plan is soon to be out of date and needs to reflect the new DR solution. The proposed cloud based Microsoft Azure Site Recovery Service is currently in design phase. The Plan is being implemented as a project and part of the project plan involves updating the legacy DR Plan.	Update the existing DR Plan in line with the proposed DR solution.	N/A
The DR Plan has been communicated to the relevant parties within the Council.	Part of the project for the new DR solution involves periodic project progress updates to senior management. Once the DR Plan has been updated, it will be communicated to relevant users within the Council.	Ensure that the existing DR Plan is updated in line with the proposed solution, approved and communicated to relevant users.	N/A
DR Plan consultation and preparation has been conducted.	DR Plan consultation for the new DR solution has not been undertaken. It was noted that consultation will be carried out as part of the new DR solution project.	Ensure that the new DR Plan consultations are carried out to ensure that all stakeholders are involved in the development of the plan.	N/A
Third party agreements relating to DR are in place and are valid	Third party agreements relating to DR are in place and are valid with the following third parties identified as key providers: • Capita – responsible for major IT services and also plays a major role in the development of the new DR solution.	N/A	N/A

	• SunGard - responsible for the primary data centre, recovery site, backup and some aspects of IT disaster recovery. • Microsoft – will provide the cloud based Microsoft Azure Site Recovery Services.		
Critical business locations, operations and or systems are identified.	Critical business locations have been identified as part of the project. The design of the new DR solution also identifies critical business locations, operations and systems and will result in the migration of data and systems to the Microsoft Azure cloud service. It is however, understood that some servers / applications will not operate in this new solution (i.e. Solaris/Sparc), and in such instances a replacement arrangement will need to be developed.	The following actions have been planned as part of the project: • Migration of servers and system to Microsoft Azure cloud service. • Replacement of servers and applications that cannot be migrated to Microsoft Azure cloud service. • Making arrangement for the backup and recovery of servers and applications that cannot be migrated to Microsoft Azure cloud service	N/A
Prioritisation of critical activities and Recovery Time Objectives have been established.	Prioritisation of critical activities and Recovery Time Objectives are contained within the Backup High Level Design and the DR High Level Designs for the new DR solution.	N/A	N/A
A formal DR risk assessment or Business Impact Assessment exercise has been conducted and documented	DR risks are covered as part of the project design and implementation of the new DR solution and a project Risk Log is also maintained.	N/A	N/A
A complete, accurate and up to date DR contact list/team has been established and is included on the DR Plan	The DR contact list and DR team has not been developed for the new DR solution. It was noted that the old DR list and DR team still applies as indicated on the old DR Plan. Part of the new DR solution project involves the update of the DR contact list and DR team.	The DR contact list and DR team should be updated to highlight the new DR solution.	N/A
Adequate Disaster Escalation and Invocation Procedures are in place.	Disaster Escalation and Invocation Procedures are still as per the old DR plan, with part of the new DR solution project involving the update of the Plans.	Disaster Escalation Procedures and Invocation Procedures should be updated in line with the new DR Solution.	N/A

Adequate emergency action procedures are in place and include Disaster Recovery.	Emergency Action Procedures are covered within the old DR Plan. The new DR solution design does not cover emergency action procedures. However, part of the new DR solution project involve the updating the existing Emergency Action Procedure. .	Emergency Action Procedures should be updated in line with the new DR Solution.	N/A
Adequate Salvage and Relocation Procedures for recovery of Items/functions which are not fully effected by the disaster are in place.	Salvage and Relocation Procedures are not in place.	N/A	Refer to finding one above under section 3.
An insurance policy for disaster recovery	An insurance policy for disaster recovery for the Council could not be provided.	N/A	Refer to finding two above under section 3.
Emergency funds have been allocated for disaster recovery.	Evidence could not be provided to verify if emergency funds have been allocated for disaster recovery.	N/A	Refer to finding two above under section 3.
DR test plans have been documented, tested, test results are documented and amendments are made to the Plan on a timely basis and test results are reported to Senior Management.	The DR test plan has been outlined on the new DR Solution Project Plan, the test plan indicates the ideal test plan for the new solution. Part of the new DR Plan project involves updating the DR plan, test plans and testing the DR plan.	IT management should ensure that once the new DR solution design and implementation is completed, the actual test plan or procedure is developed and the DR Plan is tested and test results are used to update the plan.	N/A
Backup Procedures and processes have been developed.	A Backup Procedure or Process for the new DR solution has not been developed, the old backup process still applies and part of the project plan involves updating the backup procedure.	The Backup Procedure should be updated in line with the new DR solution.	N/A
Data backups are performed and backups are securely stored offsite.	The new DR solution will provide assurance that data and systems are held in the cloud and the agreement with Microsoft requires the service provider to have an offsite copy of the backup. These processes have not been implemented as the solution is still in design.	The council should ensure that the Council's data and systems to be held by Microsoft can be made available when required.	N/A
Backups are tested for recoverability	The DR test plan including backup testing has been outlined in the new DR Solution Project Plan, the test plan indicates the ideal test plan for the new solution.	IT management should ensure that, once the new DR solution has been implemented and data and systems have been migrated to Microsoft Azure	N/A

	Part of the project for the new DR Plan includes updating the DR plan and backup procedures.	cloud services, backups are tested for recoverability.	

Appendix 2

TERMS OF REFERENCE

Backup and Disaster Recovery Audit (IT systems)

1. INTRODUCTION AND BACKGROUND

1.1 The Council's Backups and Disaster Recovery is managed by internal IT together with its IT service provider (Capita). As part of this year's plan an audit of a Backup and Disaster Recovery will be performed to ensure that backups are performed in line with business requirement and Disaster Recovery arrangements are in place and tested to ensure that the Council will be able to recover its critical data, key systems and its major business operations in the event of a disaster.

1.2 This audit is part of the Internal Audit Plan for 2017/18 as agreed by the General Purposes and Audit Committee.

2. OBJECTIVES AND METHODOLOGY

2.1 The overall audit objective of this audit is to provide an objective independent opinion on the adequacy and effectiveness of the control environment with regards Backup and Disaster Recovery (DR).

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 audit testing.

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

3. SCOPE

3.1 This audit will examine the following areas:

Disaster Recovery Procedures

- Disaster Recovery Strategy
- Plan Communication
- Third Party Agreements

Critical Business Functions and Systems

- Identification of Critical Activities
- Prioritisation of Critical Activities
- Recovery Time Objectives

Disaster Risk Assessment

- Business Impact Assessment
- Risk Assessment

Disaster Escalation and Emergency Action Procedures

- Disaster Invocation Procedure
- Incident Management Plan
- Escalation Procedure

DR Plan Updates

- Change Control Procedures for Updates
- Plan Distribution and Maintenance.

Temporary and Salvage Arrangements

DR Test Plan

- Disaster Recovery Testing, Documenting of Test Results and Reporting

Insurance cover

Backup arrangements

- Backup procedures and process
- Data Backups are Performed
- Backups are Securely Stored Offsite
- Backups are Tested for Recoverability

Appendix 3

DEFINITIONS FOR AUDIT OPINIONS AND RECOMENDATIONS

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 recommendations 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.

Appendix 4

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.

In this document references to Mazars are references to Mazars Public Sector Internal Audit Limited.

Registered office: Tower Bridge House, St Katharine's Way, London E1W 1DD, United Kingdom. Registered in England and Wales No 4585162.

Mazars Public Sector Internal Audit Limited is a subsidiary of Mazars LLP. Mazars LLP is the UK firm of Mazars, an international advisory and accountancy group. Mazars LLP is registered by the Institute of Chartered Accountants in England and Wales to carry out company audit work.