MAZARS

CROYDON

Final Internal Audit Report
Service Desk
October 2017

Distribution:

Executive Director Resources

Director of Customer and Transformation

Head of ICT & Transformation

ICT Service & Contract Manager

Assurance Level	Recommendations Made	
Substantial Assurance	Priority 1	0
	Priority 2	5
	Priority 3	0

Status of Our Reports

This report ('Report') was prepared by Mazars Public Sector Internal Audit Limited at the request of the 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 work. Whilst every care has been taken to ensure that the information provided in this Report is as accurate as possible, we 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 the London Borough of Croydon and to the fullest extent permitted by law, Mazars Public Sector Internal Audit Limited 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. Accordingly, any reliance placed on the Report, its contents, conclusions, any extract, reinterpretation, amendment and/or modification by any third party is entirely at their own risk.

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

Contents

Page

Executive Summary

1. Introduction

1.1 The Council's Service Desk, including network infrastructure, server operating system security, is managed by its IT service provider, Capita. As part of the annual audit plan, an audit of the Service Desk was performed to ensure that, a centralised Service Desk is in place. This should provide a first point of contact for users and help to facilitate the restoration of normal operational service with minimal business impact on the user, within agreed service levels and business priorities.

2. Key Issues

Priority 2 Recommendations
Service Desk Incident Procedures did not include procedures for assigning incidents, monitoring and communicating the progress of incidents, and closing of incidents. **(Rec 1).**
Review of the Service Desk application password parameters noted that, password history is not maintained and invalid login attempts are unlimited. **(Rec 2).**
Review of SLA reports against agreed SLA indicated that performance targets were not met throughout the year. **(Rec 3).**
Evidence was not provided to confirm that backup and recovery arrangements are in place for the Service Desk application. **(Rec 4).**
Evidence was not provided to verify that Service Desk application changes are performed, tested and authorised before implementation. **(Rec 5).**

3. Actions and Key Findings/Rationale

Control Area 2: Service Desk Application				
Priority	**Recommendation 1**	**Detailed Finding / Rationale**		
2	The Service Desk Incident Procedure should be reviewed and updated to include the following: • procedures for assigning incidents; • monitoring and communicating the progress of incidents; and • closing of incidents.	Having appropriately documented Service Desk Incident Procedures will ensure that incidents are consistently managed in line with business requirements. Although a documented Service Desk Incident Procedure indicating the incident classification, priority and impacts is in place, it did not cover the following: • procedures for assigning incidents; • monitoring and communicating the progress of incidents; and • closing of incidents. If documented Service Desk Incident Procedures do not include all key aspect of incident management such as procedures for assigning incidents, there is an increased risk that inconsistencies may exist, which may result in delays in resolving high priority incidents.		
Management Response		**Agreed/Disagreed**	**Responsible Officer**	**Deadline**
The procedure for assigning incidents is now: 1. Incident is logged into service now by the service desk agent 2. Incident is assigned and investigated by the service desk agent 3. If the Incident is not FTF, then it's assigned to a resolver group 4. The team lead from that resolver group assign an engineer to the incident 5. The team lead is continually checking for new incident attached to their resolver group 6. The engineer contact the user using 3 strikes rule 7. If no response after 3 strikes, the engineer inform the user that the incident will be closed. 8. If the user responds, the engineer resolves the incident and informs the user when it's been fixed. 9. The user confirms it's fixed 10. The engineer closes the incident.		Agreed	Service Delivery Manager and ICT Services & Contracts Manager	Completed

Priority	Recommendation 2	Detailed Finding / Rationale		
2	Password controls should be strengthened and aligned with the Council's security policy: • password history of at least 10 previous passwords is maintained; and • number of invalid login attempts should be set at three.	Password controls should be sufficiently robust to prevent users accessing other users' accounts and gaining inappropriate levels of system access and functionality. This includes automatic controls locking user accounts after failed login attempts and preventing the reuse of passwords (which weakens the strength of password controls). Audit review of the Service Desk application password parameters settings noted the following weak password settings are in place: • password history is not maintained; a password script check against current password only; and • number of incorrect password attempts is unlimited as auto-user lockout has not been employed. The use of weak passwords increases the risk that unauthorised access may be gained into the Service Desk application.		
Management Response		**Agreed/Disagreed**	**Responsible Officer**	**Deadline**
This recommendation will be mitigated when Capita replace the current service desk system (Service Now) with a new system called Remedy. This is due to go live in October/November 2017. With this new service desk system Capita will have the ability to change the password controls as described in the recommendation above.		Agreed	Capita Service Delivery Manager and ICT Services & Contracts Manager	October/November 2017

Control Area 3: Service Desk Performance

Priority	Recommendation 3	Detailed Finding / Rationale
2	Service Desk management should ensure that agreed SLA targets are appropriately measured and achieved.	Having an agreed SLA with achievable targets will ensure appropriate measurement of the Service Desk performance. Review of SLA reports against agreed SLA indicated that performance targets were not met throughout the year, such as the following Service Desk SLA breaches: • response times for Priority 1 incidence (response within 15 minutes), 92.27% was achieved for quarter ending September 2016, while SLA target was 100% • response times for Priority 2 incidence (response within 1 hour), 92.27% was achieved for quarter ending September 2016, while the SLA target was 100%; • telephone answer time within 20 seconds, 50.89% was achieved for quarter ending September 2015, while the SLA target was 80%; • telephone answer time within 60 seconds, 64.41% was achieved for quarter ending September 2015, while the SLA target was 80%; and • Monthly customer satisfaction surveys was last performed in April 2016, (3 months prior to the audit) while the target is one survey per month and a score of 95% from the survey. If SLA targets are not met, there is an increased risk that high priority incidents are not being addressed in time or not being addressed at all, which may result in the Council not being able to deliver key service and its IT Service provider not meeting its contractual obligations.

Management Response	Agreed/Disagreed	Responsible Officer	Deadline
At the time of the audit, it was mentioned to the auditor that the SLAs were under review because it was impossible for Capita to achieve 100% SLA. LBC & Capita are still in discussions over modifying these SLA's. Capita have now employed a breach manager who monitors incidents/requests that are due to breach and implements plans to address these.	Agreed	Service Delivery Manager and ICT Services & Contracts Manager	In progress

Control Area 4: Back-up and Recovery

Priority	Recommendation 4	Detailed Finding / Rationale
2	Service Desk management should ensure that backup and recovery arrangements are in place and cover the following areas for the Service Desk application: • updated and approved backup policy/procedure; • backups are actually performed and the logs are reviewed and retained; • backup restoration testing is performed regularly; and • an updated and approved Disaster Recovery Plan or procedures for the application is in place.	Having documented backup and recovery plans and procedures will aid the timely and adequate recovery of the Service Desk application in a recovery scenario, in line with business requirements and priorities. Ensuring that processes and responsibilities are clearly defined will aid in the efficiency and effectiveness of recovery operations. Ensuring that backups are actually performed and regularly tested for restoration purpose, will ensure that the Service Desk application data and system can be restored in the event of an incident. Evidence was not provided to confirm that the following backup and recovery arrangements are in place for the Service Desk application: • backup policy/procedure; • backups are actually performed and logs are available; • backup restoration testing is performed; and • Disaster Recovery Plan or procedures are in place. Where disaster recovery arrangements have not been formally identified and defined, and periodically tested, backups not being performed and tested for restoration, there is increased risk that the Service Desk application will not be recovered in a timely manner, should such a recovery scenario occur.

Management Response	Agreed/Disagreed	Responsible Officer	Deadline
Last year on 21/10/16 (after the audit was conducted) a BCP/DR test exercise was conducted as planned, which included our key service desk sites. Please be aware that Capita ITS currently hold ISO22301 certification (Business Continuity Standard) – and our Chippenham site recently passed a recertification visit, where BCP documentation and processes were reviewed and confirmed to meet the ISO22301 certification standard.	Agreed	Service Delivery Manager and ICT Services & Contracts Manager	Completed

Control Area 5: Support agreements and Change Control				
Priority	**Recommendation 5**	**Detailed Finding / Rationale**		
2	Management should ensure that Service Desk application changes are performed as per the Change Management procedures and ensure that evidence of changes performed, change testing and change authorisation is maintained.	Documentation of proposed changes, authorised and testing will help in ensuring that changes are performed in line with the Change Procedure and are in line with business requirements. Although a documented Change Management Procedure was in place and covered the process to be followed when implementing changes on the Service Desk application, evidence was not provided to confirm: • changes performed; • changes are tested; and • authorised before implementation. Where there is no evidence to confirm that changes are performed as per the Change Procedure, there is an increased risk that changes made to the Service Desk application, are not appropriately tested and authorised nor in line with business requirements.		
Management Response		**Agreed/Disagreed**	**Responsible Officer**	**Deadline**
The service desk tool is multi-tenant and sample of changes will not be shared with LBC for security reasons. We have already provided the formal Capita change process to the auditors.		Agreed	Service Delivery Manager and ICT Services & Contracts Manager	Completed

Appendix 1

TERMS OF REFERENCE

SERVICE DESK AUDIT

1. INTRODUCTION AND BACKGROUND

1.1 The Council's Service Desk including network infrastructure, server operating system security, is managed by its IT service provider, Capita. As part of this year's plan an audit of the Service Desk will be performed to ensure that a centralised Service Desk that provides a first point of contact for users and helps to facilitate the restoration of normal operational service with minimal business impact on the user within agreed service levels and business priorities is in place.

1.2 This audit is part of the Internal Audit Plan for 2016/17 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 Service Desk.

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:

Control Areas/Risks	Recommendations Made		
	Priority 1 (High)	Priority 2 (Medium)	Priority 3 (Low)
Service Desk Services	0	0	0
Service Desk Application	0	2	0
Service Desk Performance	0	1	0
Business Continuity and Disaster Recovery	0	1	0
Support Arrangements	0	1	0

Appendix 2

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 3

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.