MAZARS

CROYDON

Final Internal Audit Report

Wide Area Network (WAN) Connectivity

June 2017

Distribution:

Executive Director Resources (Final only)
Director Customer and Corporate Services
Head of ICT and Transformation
ICT Service & Contract Manager

Assurance Level	Recommendations Made	
Substantial Assurance	Priority 1	0
	Priority 2	2
	Priority 3	4

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

Detailed Report

Appendices

Executive Summary

1. Introduction

1.1 The Council's Wide Area Network (WAN) Connectivity services are part of the comprehensive range of managed ICT services delivered by its IT service provider, Capita Secure Information Solutions Limited.

1.2 This audit is part of the Internal Audit Plan for 2016/17. The audit objectives, methodology and scope are contained in the Audit Terms of Reference at Appendix 1.

2. Key Issues

Priority 2 Recommendations
Management should ensure that a defined network strategy that includes WAN connectivity is developed, **(Rec 1).**
Management should ensure that adequate restricted access is implemented at the Family Justice Centre, Park Lane site, **(Rec 2).**

Priority 3 recommendations are detailed under item 4.

3. Actions and Key Findings/Rationale

WAN Strategy and Support: WAN Strategy

Priority	Agreed Action/s (Recommendation 1)	Detailed Finding/Rational
2	Management should ensure that a defined network strategy, that includes WAN connectivity, is developed with main aim to support LBC in meeting its business objectives. This Strategy should also address how key network devices such as servers and switches are maintained. The strategy should identify how the network is managed and what KPI's exist to monitor network effectiveness. There should be a monitoring system for progress against the strategic plan, and subject to periodic (3-5yrs) review.	A defined strategy is vital as a proactive approach to provide long term effectiveness and sets the direction of where the organisation plans to go. Audit review identified that the Network Strategy is currently being developed and will include WAN strategy. Unless an effective and current WAN Strategy is in place, there is a significant risk that project based funding procurement decisions could be made on network devices which conflict with each other or introduce non supported technology.

Management Response	Agreed/Disagreed	Responsible Officer	Deadline
LBC senior management to review and assign an owner to work with Capita to develop a defined Network Strategy that includes WAN connectivity.	Agreed	ICT Sourcing Relationship Manager	30th June 2017

Physical Access Controls: WAN Equipment Room Access

Priority	Agreed Action/s (Recommendation 2)	Detailed Finding/Rational
2	Management should ensure that adequate restricted access is implemented at the Family Justice Centre, Park Lane site. A restricted area notice should be placed on the door. Furthermore, a combination key locker/cabinet, or a key lock box should be procured and fitted to ensure the key is stored securely.	Having a restricted access mechanisms in place will reduce the possibility of an individual accessing unauthorised areas. A visit to the Family Justice Centre, Park Lane site identified that access is not adequately restricted to the room where the WAN connectivity equipment is stored. The key to the room was left hanging in the lock, with the door unlocked and unattended. Failing to implement adequate restricted access can lead to unauthorised access resulting in loss of or damage of computer equipment through theft and foul play.

Management Response	Agreed/Disagreed	Responsible Officer	Deadline
There is a low likelihood of inappropriate access (due to building access controls) and the mitigations available for any impact due to no servers being located onsite. With the assistance of Facilities Management, a restricted area notice has now been placed on the door and a key lock box has been procured and fitted for the secure storage of the key. It should be noted that whilst the public do access the building, this access is controlled by reception staff by way of a buzzer. The IT room only contains the entry point for the building's internet connection along with its WAN switches. There are no servers with data located in this IT room. Any disruption to equipment in the room would only	Agreed	ICT Service & Contract Manager	Completed

impair connectivity locally and this would be mitigated by standard business continuity plans. Our ICT infrastructure allows remote access to the LBC network provided there is an internet connection – as such any loss of connectivity could be temporarily mitigated through the provision of e.g. a 4G dongle or MIFI hub.			

4. Priority 3 Recommendations

Agreed Action/s	Detailed Finding / Rationale
1. Management should ensure that all ICT policy documents are reviewed and approved by senior management. They should be reviewed periodically and updated to ensure they reflect the actual processes taking place and fit for purpose.	While there are written policies and procedures, review of the policy documents, for example, IT Access Policy, ICT Infrastructure Security Policy, Email Electronic Messaging and Internet Policy, etc., identified that these have not been reviewed or updated since 2012. Where key policies have not been formally documented, reviewed and/or approved, the information contained within these may be out of date, irrelevant and not fit for purpose.
2. Management should ensure that a burglar alarm system is installed at the Family Justice Centre, Park Lane site. The burglar alarm system may include but not limited to a number of sensors that detect intrusion such as, motion detectors, contact sensors, thermal detectors, glass breakage detectors, and weight sensors.	Observation of the Family Justice Centre, Park Lane site identified that there is no adequate burglar alarm system in place. Failing to implement an adequate burglar alarm system may lead to intrusion into unauthorised areas going unnoticed resulting in theft and loss of data.
3. Management should ensure that the computer rooms are kept clean and tidy at all times.	Observation of the three sites identified that the rooms were used as storage with card boxes and cleaning equipment. Failing to keep the rooms clean and tidy increases the risk of trips, falls and fire hazards.
4. Management should ensure that there is adequate systems in place to prevent water damage to the WAN connectivity equipment in the network rooms. This should include, but not limited to, installation of water detection sensors, water drains.	Observation of the Family Justice Centre, Park Lane site identified that there is no water pipe in the room, however, there was no water drainage or detection sensors installed. Failing to implement an adequate system to prevent water damage may lead to damage to the IT equipment resulting in loss of data.

Appendix 1

TERMS OF REFERENCE

WAN Connectivity Audit

1. INTRODUCTION AND BACKGROUND

1.1 The Council's Wide Area Network (WAN) Connectivity services are part of the comprehensive range of managed ICT services delivered by its IT service provider, Capita Secure Information Solutions Limited.

1.2 This audit is part of the agreed Internal Audit Plan for 2016/17. It will ensure the network infrastructure have effective physical security and access controls to protect network resources. In addition, review whether network components provide adequate network security and review management structure is in place to facilitate the restoration of normal operational service with minimal business impact on the user within agreed service levels and business priorities.

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 to WAN Connectivity; that this supports and promotes the achievement of the Council's service objectives.

2.2 In order to achieve the overall objectives, a risk-based system 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 examined the following areas, (as these relate to WAN connectivity):

Control Areas/Risks	Recommendations Made		
	Priority 1 (High)	Priority 2 (Medium)	Priority 3 (Low)
WAN and Corporate Strategy	0	1	1
Network Infrastructure and Design	0	0	0
Network Management and Monitoring	0	0	0
Logical Security and Encryption	0	0	0
Physical Access Controls	0	1	3
Environmental Controls	0	0	0

Backup, Disaster Recovery and Contingency Plans	0	0	0
Change Controls	0	0	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.

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 Public Sector Internal Audit Limited accepts no responsibility and disclaims all liability to any third party who purports to use or reply 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.

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.