MAZARS

CROYDON

Final Internal Audit Report

Citrix Security

August 2017

Distribution:

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

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

Detailed Report

Appendices

Executive Summary

1. Introduction

1.1 Citrix solutions provides a platform that allows the individual users of an enterprise to work and collaborate remotely in a virtual computer environment regardless of device or network. The deployment of secure and effective Citrix technology solutions helps to maximise system efficiency and to minimise the risks to system availability, integrity and availability.

1.2 Capita, the Council's IT Service provider, is currently in the process of using Citrix solutions in the roll out to the Council's virtual desktop estate as part of its technical refresh programme.

1.3 The General Purposes and Audit Committee agreed the Internal Audit Plan for 2016/17 on the 23 March 2016. As part of that plan, an internal audit in respect of Citrix security was identified to be undertaken.

2. Key Issues

Priority 2 Recommendations
While Capita has completed and documented the results of their Citrix security configuration tests, the configuration settings are yet to be formally evaluated against the vendor's best practice standards and signed off by the ICT Client Unit, **(Rec 1).**
Capita has completed and documented the results of their Citrix performance loading tests to help establish and agree upon the appropriate capacity management thresholds to be monitored via the Citrix Director Console management tools and reports. However, it was identified that, as yet, no Key Performance Indicator (KPI) monitoring reports are in place to help the ICT Client Unit to monitor and keep track of the ongoing Citrix Security Patch Management activities **(Rec 2).**

3. Actions and Key Findings/Rationale

Secure Citrix Configuration: Citrix Technical Security Configuration Settings

Priority	Agreed Action/s (Recommendation 1)	Detailed Finding/Rational
2	The ICT Client Unit should formally: a) evaluate and assess the results of the documented security tests; and b) compare the Citrix security settings against an appropriate Citrix security hardening guide.	Formal assessment of the Citrix security tests conducted by Capita and agreement upon the use of appropriate Citrix security configuration settings helps the Council to ensure that effective Citrix security controls have been established and applied. Discussions with the Council's ICT Client Unit (ICU) and Capita identified that, although Capita has completed a range of Citrix security and performance evaluation tests to help ensure that appropriate capacity monitoring thresholds are established and applied, the ICT Client Unit has yet to formally assess and agree upon the use of the Citrix security settings against an appropriate Citrix security hardening guide. Until the ICT Client Unit has formally evaluated the results of the Citrix Security and performance evaluation tests that have been completed by Capita, there is a risk that the Citrix security configuration settings may not meet the Council's requirements. This could result in inappropriate policies being applied, the devices not working or performing as expected or could potentially have vulnerabilities that could ultimately expose security weaknesses in the Council's network.

Management Response	Agreed/Disagreed	Responsible Officer	Deadline
The recommendations will be implemented.	Agreed	Enterprise Architect	31st August 2017

Citrix Monitoring: Citrix Performance Monitoring

Priority	Agreed Action/s (Recommendation 2)	Detailed Finding/Rational
2	The ICT Client Unit should ensure that appropriate key performance indicators are established and applied to assist them in monitoring the frequency and effectiveness of the Citrix patch handling utility (cpatch.exe) which is used for installation and removal of Citrix patches, such as service packs and security patch hotfixes.	Formal assessment of appropriate Citrix security patch management activities helps to ensure that the recommended and prioritised Citrix patches, such as service packs and security hotfixes, are being identified and applied in a timely manner. Discussions with the Council's ICT Client Unit (ICU) and Capita identified that no key performance indicator management reports are currently in use to assist the ICT Client Unit in monitoring the frequency and effectiveness of the Citrix security patch management activities. Until appropriate key performance indicators and monitoring arrangements are established for Citrix security patch management activities, there is an increased risk that patch management activities could be ineffective and go undetected. This could result in inappropriate security patch management policies being applied and leave known vulnerabilities unaddressed that could be used to exploit security weakness in the Council's network.

Management Response	Agreed/Disagreed	Responsible Officer	Deadline
LBC have requested Capita to provide performance measurements on the Citrix patch handling as part of the monthly capacity report and service report. In addition to this, a review with LBC/Capita is currently underway on the complete patch management cycle which incorporates reporting that highlights the effectiveness of the patching process.	Agreed	Service Delivery Manager - Capita IT Enterprise Services	31 August 2017

Appendix 1

TERMS OF REFERENCE

CITRIX SECURITY AUDIT

1. INTRODUCTION

1.1 The deployment of secure and effective Citrix technology solutions helps to maximise system efficiency and to minimise the risks to system availability, integrity and availability.

1.2 This audit is part of the Internal Audit Plan for 2016/17 and agreed by the General Purposes and Audit Committee.

2. OBJECTIVES AND METHOD

2.1 The overall audit objective is to provide an objective independent opinion on the adequacy and effectiveness of the control framework established and applied to the deployment and management of secure and effective Citrix technology solutions and activity monitoring arrangements.

2.2 The audit will for each controls / process being considered:

- Document and evaluate the processes to consider the key risks and controls;
- Undertake sufficient testing of controls operating, on a sample basis, and
- Reach a conclusion of the effectiveness of controls operating and report

3. SCOPE

3.1 This audit will evaluate the Citrix technology control environment by examination of the controls applied to help manage and mitigate risks in the following areas:

Control Areas/Risks	Recommendations Made		
	Priority 1 (High)	Priority 2 (Medium)	Priority 3 (Low)
Governance Roles and Responsibilities	0	0	0
System Resilience	0	0	0
Citrix System Security Settings	0	1	0
Citrix System Monitoring Reports	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.

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.