

Oxford City Council

INTERNAL AUDIT REPORT

Cyber Crime

81

May 2017

LEVEL OF ASSURANCE	
Design	Operational Effectiveness
Moderate	Limited



CONTENTS

Executive Summary	3
Detailed Findings and Recommendations	4
Appendices:	
I Staff Interviewed	12
II Definitions	13
III Terms of Reference	14

82

REPORT STATUS	
Auditors:	David Harvey, IT Audit Manager
Dates work performed:	April 2017
Draft report issued:	April 2017
Final report issued:	May 2017

DISTRIBUTION LIST	
Jackie Yates	Executive Director for Organisational Development and Communication
Nigel Kennedy	Section 151 Officer
Helen Bishop	Head of Business Development
Vic Frewin	Head of ICT
Michael Ngero	Information Governance Manager

Restrictions of use

The matters raised in this report are only those which came to our attention during the course of our audit and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. The report has been prepared solely for the management of the organisation and should not be quoted in whole or in part without our prior written consent. BDO LLP neither owes nor accepts any duty to any third party whether in contract or in tort and shall not be liable, in respect of any loss, damage or expense which is caused by their reliance on this report.

EXECUTIVE SUMMARY

CLIENT STRATEGIC RISKS			SUMMARY OF RECOMMENDATIONS (SEE APPENDIX II FOR DEFINITIONS)	
Risk	The Council's services are disrupted as a result of a cyber security incident.		High	1
LEVEL OF ASSURANCE (SEE APPENDIX II FOR DEFINITIONS)			Medium	6
Design	Moderate	Generally a sound system of internal control designed to achieve system objectives with some exceptions.	Low	1
Effectiveness	Limited	Non-compliance with key procedures and controls places the system objectives at risk.	Total number of recommendations: 8	

OVERVIEW

The purpose of our review was to appraise the design and effectiveness of the Council's procedures for identifying and protecting its information assets from a cyber security attack and for managing its cyber security risks on an ongoing basis. Vulnerabilities in the technology that is used to process personal information, and in the associated processes, can be exploited by an attacker, compromising the Council's information assets and causing significant financial and reputational damage. The Council's IT infrastructure is provided and managed by SCC, whilst the ICT department is responsible for the management of endpoint devices such as laptops.

The following areas of good practice were identified:

- ICT routinely provide members of staff with updates regarding data protection, information security and cyber security
- Responsibility for information and cyber security management has been assigned to a named member of staff
- The IT network diagram records the network perimeter security controls that have been deployed.

However, we identified the following areas of improvement:

- Operating system patches have not been applied to the Council's endpoint devices such as desktop and laptop computers. This has now been resolved (Finding 1 - High)
- The Information Security policy does not include all relevant information and is not reflective of existing arrangements (Finding 2 - Medium)
- The Information Asset Register was found to be incomplete (Finding 3 - Medium)
- Members of staff are not provided with adequate information and cyber security training (Finding 4 - Medium)
- SCC has not provided the Council with sufficient assurances as to the efficacy of its network perimeter security controls. The Council has now initiated conversations with SCC on this matter (Finding 5- Medium)
- The Council does not have the ability to review the configuration and operation of its firewall ruleset. As per finding five, the Council has now initiated conversations with SCC on this matter (Finding 6 - Medium)
- A disproportionately high number of members of staff have been granted domain administrator permissions. The Council has commenced a review of domain administrator rights and has asked SCC to clarify the need for these accounts going forward. (Finding 7 - Medium)

EXECUTIVE SUMMARY

OVERVIEW (cont.)

ICT, in conjunction with SCC, have taken appropriate action to design appropriate controls to protect the Council's information assets from a cyber-attack. However, weaknesses were identified in the operational efficacy of these controls that, if exploited, could result in a breach occurring. Consequently, we conclude moderate assurance as to the design of the controls and limited assurance as to the effectiveness.

DETAILED RECOMMENDATIONS

RISK: Network security controls are not reviewed on a routine basis			
Ref.	Finding	Sig.	Recommendation
1	<p>The ICT department are responsible for the review, testing and deployment of operating system patches for the Council's endpoint devices, such as desktop and laptop computers.</p> <p>We found that operating system patches have not been deployed to endpoint devices following the transition of IT services from Oxfordshire County Council in April 2016. Whilst a patching schedule is being developed, this has not been implemented.</p> <p>Furthermore, there is not a standard operating procedure in place for applying operating system patches following their release by the developer.</p> <p>Not applying operating system patches as and when they are released by the developer increases the risk of vulnerabilities being exploited in order to gain unauthorised access to the IT network.</p>	High	<p>Management must establish a standard operating procedure for applying operating system patches to the Council's endpoint devices as and when they are released by the Developer.</p> <p>The patching status of the Council's IT estate should be reviewed on a routine basis.</p>
MANAGEMENT RESPONSE			RESPONSIBILITY AND IMPLEMENTATION DATE
<p>Agreed - This has now been addressed and a patch management process is now in place. The Microsoft release for April has been applied to the Council's IT estate.</p>			<p>Responsible Officer: Vic Frewin, Interim CTO Implementation Date: Closed</p>

85

DETAILED RECOMMENDATIONS

RISK: Threats to the Council are not adequately identified nor are there procedures in place to prevent vulnerabilities being exploited			
Ref.	Finding	Sig.	Recommendation
2	<p>The Council's Information Security policy has not been reviewed since it was issued in November 2014. We found that the Policy is not reflective of existing ways of working within the Council and does not include:</p> <ul style="list-style-type: none"> • The responsibilities of stakeholders across the Council with regards to information security, including information asset owners • The relationship and arrangements that exist between the Council and its IT provider, SCC • The Council's procedures for classifying information in line with the Government Security Classification policy • The Council's acceptable use standards • The actions to be taken by ICT and SCC when responding to an information security incident. <p>Not reviewing the Information Security policy on a routine basis increases the risk of the policy being incomplete and inaccurate.</p>	Med	<p>Management should review and, where necessary, revise the Council's Information Security policy so that it is reflective of existing ways of working. The policy should include, but not be limited to:</p> <ul style="list-style-type: none"> • The responsibilities of all stakeholders with regards to information security, including information asset owners • The roles, responsibilities and arrangements that exist between the Council and SCC • The procedure for classifying information assets • The Council's acceptable use standards • The actions to be taken by all parties following the identification of an information security incident.
MANAGEMENT RESPONSE			RESPONSIBILITY AND IMPLEMENTATION DATE
Agreed - The policy will be reviewed and updated.			<p>Responsible Officer: Vic Frewin, Interim CTO Implementation Date: October 2017</p>

86

DETAILED RECOMMENDATIONS

RISK: There are inadequate procedures in place to classify and secure the Council's information security assets			
Ref.	Finding	Sig.	Recommendation
3	<p>It was observed during our fieldwork that the Council's Information Asset Register was in draft pending approval from Senior Management and the identified Information Asset Owners. Our review of the draft Information Asset Register found that:</p> <ul style="list-style-type: none"> • It does not record the security controls that have been applied to each information asset • The at-rest location for each information asset has not been recorded • The classifications applied to each information asset are not consistent with the Government Security Classification Standard • There are a number of information assets that have incomplete entries. <p>The absence of a defined information asset register increases the risk of a breach as a result of insufficient or inadequate security controls.</p>	Med	<p>The Council's draft Information Asset Register should be updated to include:</p> <ul style="list-style-type: none"> • The security controls that have been applied to secure each information asset • The at-rest location of each information asset • The classification applied to each information asset, in line with the Council's and the Government's Security Classification standards. <p>All required information should be recorded for each information asset.</p> <p>The Information Asset Register should be reviewed and approved by Senior Management and then communicated to all relevant stakeholders.</p>
MANAGEMENT RESPONSE		RESPONSIBILITY AND IMPLEMENTATION DATE	
Agreed - The Information Asset Register will be completed and submitted for approval.		<p>Responsible Officer: Vic Frewin, Interim CTO Implementation Date: October 2017</p>	

87

DETAILED RECOMMENDATIONS

RISK: Threats to the Council are not adequately identified nor are there procedures in place to prevent vulnerabilities being exploited			
Ref.	Finding	Sig.	Recommendation
4	<p>All members of staff are required to complete a data protection e-learning course upon joining the Council. We found that whilst the course does reference information security it does not include:</p> <ul style="list-style-type: none"> • Guidance on how members of staff can prevent an incident from occurring such as phishing attacks or spoof emails • The actions that should be taken when an information security breach occurs. <p>The absence of appropriate information security training increases the risk of a breach occurring as a result of the actions of a member of staff.</p>	Med	<p>The training that is provided to all members of staff should be reviewed and updated so that it makes specific reference to information and cyber security issues. This should include, but not be limited to:</p> <ul style="list-style-type: none"> • How to prevent an incident from occurring, such as not responding to emails from unknown or untrusted sources • The actions to be taken when a breach is detected.
MANAGEMENT RESPONSE			RESPONSIBILITY AND IMPLEMENTATION DATE
Agreed - the provision for training will be reviewed.			<p>Responsible Officer: Vic Frewin, Interim CTO Implementation Date: October 2017</p>



DETAILED RECOMMENDATIONS

RISK: Network security controls are not reviewed on a routine basis			
Ref.	Finding	Sig.	Recommendation
5	<p>It was observed during our fieldwork that the SCC has provided the Council with assurance that its operations are compliant with the requirements of the Public Services Network (PSN) and ISO27001.</p> <p>However, these are point in time assessments and the Council is not provided with evidence to demonstrate that network perimeter security controls are reviewed on a routine basis and are operating effectively.</p> <p>Not providing the Council with assurance that SCC are performing network perimeter security controls on a routine basis increases the risk of vulnerabilities being exploited in order to gain access to the Council's IT network.</p>	Med	<p>Management should request that SCC provide routine reporting regarding the efficacy of its network perimeter security controls. This should include, but not be limited to:</p> <ul style="list-style-type: none"> • The number of information or cyber security incidents encountered and the actions taken by SCC to resolve them • The devices that have or have attempted to connect to the Council's IT network • Unusual or suspicious activity that has been detected and requires further investigation.
MANAGEMENT RESPONSE		RESPONSIBILITY AND IMPLEMENTATION DATE	
Agreed - This will be discussed within the Council and raised with SCC		<p>Responsible Officer: Vic Frewin, Interim CTO</p> <p>Implementation Date: August 2017</p>	

68

DETAILED RECOMMENDATIONS

RISK:			
Ref.	Finding	Sig.	Recommendation
6	<p>The Council’s internal and external firewalls are managed by SCC. It was observed during our fieldwork that SCC has restricted the Council’s ability to review the configuration of its firewall ruleset.</p> <p>Whilst the Council’s ICT department has been provided a .txt file that includes the firewall ruleset, it will require significant effort to be expended to translate it into a legible format and will not allow the traffic to be monitored in real-time.</p> <p>Furthermore, the firewall ruleset was migrated to SCC as part of the transition from Oxford County Council and has not been reviewed after the initial transition to determine whether it remains appropriate.</p> <p>Not reviewing the firewall ruleset on a routine basis increases the risk of unnecessary or inappropriate rules being exploited to gain unauthorised access to the Council’s IT network.</p>	Med	<p>With the assistance of SCC, the Council’s firewalls should be reviewed and, where necessary, inappropriate or unnecessary rules should be removed.</p> <p>Furthermore, management should put in place a standard operating procedure for reviewing the Council’s firewall rules on a routine basis. Where necessary, relevant information must be provided by SCC to support these reviews.</p>
MANAGEMENT RESPONSE			RESPONSIBILITY AND IMPLEMENTATION DATE
Agreed - This will be discussed and raised with SCC.			<p>Responsible Officer: Vic Frewin, Interim CTO</p> <p>Implementation Date: August 2017</p>

06

DETAILED RECOMMENDATIONS

RISK:			
Ref.	Finding	Sig.	Recommendation
7	<p>It was observed during our fieldwork that there is a disproportionately high number of user accounts that have been granted domain administrator permissions. We found that, at the time of the review, there were 84 accounts that had domain administrator permissions</p> <p>Accounts that are domain administrators have the ability to control all devices within a domain, which includes servers and computers.</p> <p>Not restricting the number of users with elevated permissions increases the risk of users gaining unauthorised access.</p>	Med	<p>Management should review and, where necessary, restrict the number of users that have been granted domain administrator access to approved users only. A record of authorised accounts should be maintained and reviewed on a routine basis.</p> <p>Furthermore, there should be a standard operating procedure in place for requesting and approving the granting of domain administrator permissions.</p>
MANAGEMENT RESPONSE			RESPONSIBILITY AND IMPLEMENTATION DATE
<p>Agreed - A review has been carried out and 40 accounts have been closed. The Council have written to SCC to clarify the purpose for their domain administrator accounts.</p>			<p>Responsible Officer: Vic Frewin, Interim CTO Implementation Date: September 2017</p>

91

DETAILED RECOMMENDATIONS

RISK:			
Ref.	Finding	Sig.	Recommendation
8	<p>It was observed during our fieldwork that the Council does not have a defined Board or Group in place to allow for information and cyber security issues to be raised with Senior Management on a routine basis.</p> <p>The absence of an information governance or security group increases the risk that members of staff, including senior management, are not made aware of information and cyber security issues.</p>	Low	Management should establish an information governance group, which includes stakeholders from the Council's senior management, to review information and cyber security issues on a routine basis.
MANAGEMENT RESPONSE			RESPONSIBILITY AND IMPLEMENTATION DATE
Agreed The Council will determine an appropriate forum for this issue to be discussed.			<p><i>Responsible Officer:</i> Vic Frewin, Interim CTO</p> <p><i>Implementation Date:</i> October 2017</p>

92

APPENDIX I - STAFF INTERVIEWED

BDO LLP appreciates the time provided by all the individuals involved in this review and would like to thank them for their assistance and cooperation.

NAME	JOB TITLE
Vic Frewin	Head of ICT
Michael Ngero	Information Governance Manager
Jon Petre	ICT Operations Manager
John Galbraith	Network Lead

APPENDIX II - DEFINITIONS

94

LEVEL OF ASSURANCE	DESIGN of internal control framework		OPERATIONAL EFFECTIVENESS of internal controls	
	Findings from review	Design Opinion	Findings from review	Effectiveness Opinion
Substantial	Appropriate procedures and controls in place to mitigate the key risks.	There is a sound system of internal control designed to achieve system objectives.	No, or only minor, exceptions found in testing of the procedures and controls.	The controls that are in place are being consistently applied.
Moderate	In the main there are appropriate procedures and controls in place to mitigate the key risks reviewed albeit with some that are not fully effective.	Generally a sound system of internal control designed to achieve system objectives with some exceptions.	A small number of exceptions found in testing of the procedures and controls.	Evidence of non compliance with some controls, that may put some of the system objectives at risk.
Limited	A number of significant gaps identified in the procedures and controls in key areas. Where practical, efforts should be made to address in-year.	System of internal controls is weakened with system objectives at risk of not being achieved.	A number of reoccurring exceptions found in testing of the procedures and controls. Where practical, efforts should be made to address in-year.	Non-compliance with key procedures and controls places the system objectives at risk.
No	For all risk areas there are significant gaps in the procedures and controls. Failure to address in-year affects the quality of the organisation's overall internal control framework.	Poor system of internal control.	Due to absence of effective controls and procedures, no reliance can be placed on their operation. Failure to address in-year affects the quality of the organisation's overall internal control framework.	Non compliance and/or compliance with inadequate controls.

Recommendation Significance	
High	A weakness where there is substantial risk of loss, fraud, impropriety, poor value for money, or failure to achieve organisational objectives. Such risk could lead to an adverse impact on the business. Remedial action must be taken urgently.
Medium	A weakness in control which, although not fundamental, relates to shortcomings which expose individual business systems to a less immediate level of threatening risk or poor value for money. Such a risk could impact on operational objectives and should be of concern to senior management and requires prompt specific action.
Low	Areas that individually have no significant impact, but where management would benefit from improved controls and/or have the opportunity to achieve greater effectiveness and/or efficiency.

APPENDIX III - TERMS OF REFERENCE

BACKGROUND



The drive to improve the efficacy and efficiency of the Council's services has resulted in the increased use of IT systems to collect, process and store personal and sensitive information. The vulnerabilities that exist in these IT systems, as well as the infrastructure that supports them, combined with a perceived lack of awareness regarding security issues has led to criminals targeting local authorities. An attack can be launched from any where in the world and can be instigated at the behest of a criminal, a politician or a disgruntled employee. As recent examples across the public sector have demonstrated, the impact of a cyber attack can have a significant financial and reputational impact.

PURPOSE OF REVIEW



This audit will appraise the design and effectiveness of the Council's procedures for identifying and protecting its information assets, and managing its cyber security risks on an ongoing basis. Our work is designed to provide an assessment of the information security and cyber crime prevention arrangements but cannot provide absolute assurance that the Council would withstand an attack on its systems

95

SCOPE OF REVIEW



This review will consider the following areas of scope:

- The Council has identified and assessed its information assets
- Security threats to the Council have been identified, assessed and action has been taken to prevent known vulnerabilities from being exploited
- Members of staff are provided with adequate training and awareness
- Appropriate network security controls have been deployed and are operational
- Access to privileged network accounts has been restricted
- There are defined incident and post-incident management arrangements in place.

EXCLUSIONS



Our work will be restricted to the areas of consideration within our scope of the review and all testing will be on a sample basis only.

APPROACH



Our approach will be to conduct interviews to establish the controls in operation for each of our areas of audit work. We will then seek documentary evidence that these controls are designed as described and will evaluate whether they adequately address the risks. As part of this audit we will require evidence from the Council's third party IT provider SCC.

APPENDIX III - TERMS OF REFERENCE

KEY RISKS

Based upon the risk assessment undertaken during the development of the internal audit operational plan, through discussions with management, and our collective audit knowledge and understanding the key risks associated with the area under review are:

- There are inadequate procedures in place to classify and secure the Council's information security assets
- Threats to the Council are not adequately identified nor are there procedures in place to prevent vulnerabilities being exploited
- Critical services provided by the Council could be disrupted in the event of a cyber attack
- Network security controls are not reviewed on a routine basis
- The Council's reputation could be negatively impacted following a successful cyber security attack.

DOCUMENTATION REQUEST

Please could appropriate members of staff complete the self-assessment form provided and return it to us ahead of the scheduled start date of the audit.

Any documents provided will assist the timely completion of our fieldwork, however we may need to request further documentation and evidence as we progress through the review process.

APPENDIX III - TERMS OF REFERENCE

TIMETABLE


Audit Stage	Date
Commence fieldwork	17 April 2017
Number of audit days planned	14
Planned date for closing meeting	1 May 2017
Planned date for issue of the draft report	5 May 2017
Planned date for receipt of management responses	19 May 2017
Planned date for issue of proposed final report	22 May 2017
Planned Audit Committee date for presentation of report	TBC


KEY CONTACTS

97

BDO LLP	Role	Telephone and/or email
Greg Rubins	Head of Internal Audit	t: 07583 114 121 e: greg.rubins@bdo.co.uk
Gurpreet Dulay	Internal Audit Manager	t: 07870 555 214 e: gurpreet.dulay@bdo.co.uk
David Harvey	Internal Audit Assistant Manager	t: 07583 179 755 e: david.harvey@bdo.co.uk
Oxford City Council		
Helen Bishop	Head of Business Development	
Vic Frewin	Head of ICT	
Nigel Kennedy	Section 151 Officer	
Jackie Yates	Executive Director for Organisational Development and Communication	

SIGN OFF


On behalf of BDO LLP:		On behalf of Oxford City Council:	
Signature:		Signature:	NIGEL KENNEDY
Title:	HEAD OF INTERNAL AUDIT	Title:	SECTION 151 OFFICER
Date:	17 March 2017	Date:	



BDO LLP, a UK limited liability partnership registered in England and Wales under number OC305127, is a member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. A list of members' names is open to inspection at our registered office, 55 Baker Street, London W1U 7EU. BDO LLP is authorised and regulated by the Financial Conduct Authority to conduct investment business.

BDO is the brand name of the BDO network and for each of the BDO Member Firms.

BDO Northern Ireland, a partnership formed in and under the laws of Northern Ireland, is licensed to operate within the international BDO network of independent member firms.

 Copyright ©2017 BDO LLP. All rights reserved.

www.bdo.co.uk

