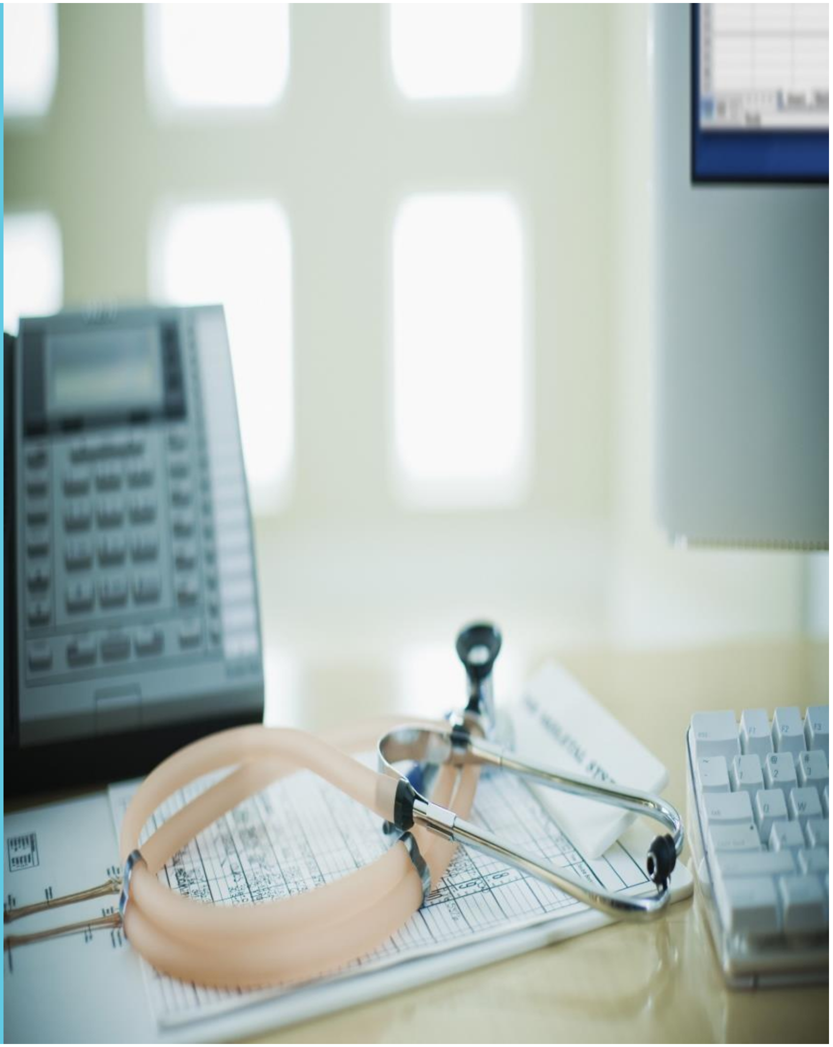
Oxford City Council

INTERNAL AUDIT REPORT

Business Improvement and Technology - System Interfaces

May 2016

LEVEL OF ASSURANCE	
Design	Operational Effectiveness
Limited	Moderate



BDO

Agenda Item 12a

CONTENTS

Appendices:

REPORT STATUS	
Auditors:	Tom Delaney
Dates work performed:	18 April 2016 - 18 May 2016
Draft report issued:	24 May 2016
Final report issued:	17 June 2016

DISTRIBUTION LIST	
Jackie Yates	Executive Director for Organisational Development and Communications
Helen Bishop	Head of Business Improvement
Paul Fleming	Chief Technology Manager
Nigel Kennedy	Section 151 Officer

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	
Risk	An Efficient and Effective Council: A customer-focused organisation, delivering efficient, high-quality services that meet people's needs.

LEVEL OF ASSURANCE (SEE APPENDIX II FOR DEFINITIONS)		
Design	Limited	System of internal controls is weakened with system objectives at risk of not being achieved.
Effectiveness	Moderate	Evidence of non compliance with some controls, that may put some of the system objectives at risk.

SUMMARY OF RECOMMENDATIONS (SEE APPENDIX II FOR DEFINITIONS)	
High	
Medium	5
Low	-
Total number of recommendations: 5	

OVERVIEW

Background

Oxford City Council (the 'Council') utilise many IT applications to support the delivery of their objectives. These applications and the data held on them must be held securely to minimise manipulation of data, interface with each other to support successful transfer of information and be upgraded/tested to ensure they are fit for purpose. From 1st April we have migrated the management of the City's ICT infrastructure to SCC, bringing the first line support back in house. This alters the shape and focus of the service from what was delivered previously.

Good Practice

- The client engages a third party to perform annual penetration testing on the Council's network, which is a proactive approach to identifying potential vulnerabilities. For any weaknesses identified, an action plan is put in place to, where practicable, undertake mitigating actions
- Those staff interviewed, both within IT and those in the wider operational roles had a strong knowledge of their role and the associated risks.

The Council are in the process of engaging SOCITM to review the work we have done so far in setting up our new structure, systems and processes. In addition, we have started to pull together our own plan to improve our service offering. This will include activities regarding:

- Vision for the service
- Developing the service management platform and reviewing and developing processes
- Developing customer service and performance management of the service and individuals (including training and management development).

However, the following areas for improvement are identified

- Management should document and communicate a process for raising, handling and escalating incidents (Finding 1 – Medium)
- Management should develop a suite of management information for reporting to senior management (Finding 1 – Medium)
- 'Multi skilled' to ensure continuity of service and/or applications support (Finding 2 – Medium)
- The user access management process (to include, new starters, internal moves and leavers) should be reviewed and guidance produced to act as a directive control and to promote consistency across the different applications (Finding 3 – Medium)
- There is no system audit trail activated in order to provide a mechanism of tracing whether inappropriate action has been taken by those with privileged user access (Finding 4 – Medium)
- Current scripts should be enhanced to enable automated alerts to be generated in the event of issues with interface failures (Finding 5 – Medium).

Conclusion

We have issued 5 medium recommendations. We have concluded the design is limited as there are not embedded controls around escalating incidents. The effectiveness is considered moderate as the controls when designed operated well.

DETAILED RECOMMENDATIONS

RISK: When the cases are subject to a 'near-miss events' for applications held, lessons are not captured and learned to support continuous learning

Ref.	Finding	Sig.	Recommendation
1	It was confirmed by the Chief Technology Manager that there is no formal documentation or process for raising, handling and escalating incidents at present as it is built into the ITSM vFire solution. This system is not fully embedded as staff are not consistently applying the capabilities of the workflow in the system. Through interviews with other staff members, it was identified that there is no clearly defined process that they are all aware of, nor do they consistently apply an approach. The theme from interviews was that it is handled on a case by case basis. As Council staff and management are aware, there have been recent incidents regarding IT interfaces, for example: • In April where a 'technical' glitch resulted in rents being taken twice from residents. This was flagged and £314,000 had to be returned to residents. This was done within a 4 hour period so no-one was impacted with a financial loss; however, it caused reputational damage. Through discussions with the IT support Analyst who was involved in the incident, it was advised that the error was due to a manual intervention in the process. Additionally, it helped to highlight an issue with one of the scripts whereby two reconciliations were being made from the same source meaning that there would never be an imbalance. The script has been fixed and no issues have been identified since.	Med	We recommend that management document and communicate a process for raising, handling and escalating incidents, and as a minimum, provide examples of incidents that may be deemed as low, medium or high in importance and the resulting process and timeframes that would follow. Where third party involvement is required, information around the process, timeframes and escalation routes should also be included in the guidance. Further to the above, we recommend that management develop a suite of management information for reporting to senior management, including incident management. This could potentially detail the results of any trend analysis that has been performed by management.

(Continued on next page)

DETAILED RECOMMENDATIONS

RISK: When the cases are subject to a ‘near-miss events’ for applications held, lessons are not captured and learned to support continuous learning			
Ref.	**Finding**	**Sig.**	**Recommendation**
1	*(Continued)* • Additionally, since the transition of services from Oxfordshire County Council to Oxford City Council, there have been incidents where data transfers have been blocked due to the different configurations of the City Council’s firewalls to that of the County firewalls. Management have confirmed that all incidents identified to date have been corrected; however, at this point there is no guarantee that the issue will not re-occur. We acknowledge that there can not be a strict 'one size fits all' approach; however, without clear guidance as to the basic steps to follow, there is a risk that the lack of awareness of procedures or the timeliness of escalation may impact on the overall resolution. Alternatively, staff outside of IT may not be aware of the process and fail to escalate. Further to the above, it was identified that for those incidents that are raised and dealt with, there is limited management information provided to senior management in terms of themes and trends of past incidents or lessons that have been learnt. Without this, there is a risk that senior management do not get oversight of incidents that could impact on the operations or reputation of the Council.	Med	
MANAGEMENT RESPONSE			**RESPONSIBILITY AND IMPLEMENTATION DATE**

DETAILED RECOMMENDATIONS

Agreed. ICT will develop a Service Level Agreement that will document high, medium and low level incidents and service requesters with respective time frames. To support this there will be the relevant management information. This will be done by 31.07.16.

The following is already in place since 1st April as mitigation:

- senior managers from ICT and Business Development allocated to service areas, regular meetings between these representatives and liaising with the service head and their management teams on a regular basis to ensure ICT is aware of all issues and priorities for attention;
- Weekly ICT update on the level of calls outstanding and progress with the major underlying issues;
- Regular intranet updates;
- Rigorous call allocation by ICT Senior Managers to the team, so there is overview of the issues logged;
- Daily ICT and Business Development Management meetings to ensure all staff are kept in the loop of the agreed action plan, issues outstanding and progress;
- Daily technical call to SCC (our infrastructure provider) to escalate issues to ensure a speedy response.

Responsible Officer:

Chief Technology and Information Manager

Implementation Date: July 2016

DETAILED RECOMMENDATIONS

RISK: Inadequate systems knowledge and training for those who manage interfaces to ensure data is properly secured and managed			
Ref.	Finding	Sig.	Recommendation
2	It was identified that the current applications support staff have not documented any processes and other staff are not generally involved in the process. Through audit interviews with the IT Support staff, it was advised that they feel that others may be able to pick up the basics but would not be able to pick up all elements of the role as there is no guidance or specific training. Further to this, it was observed through the review that the team rely heavily on the knowledge, skills and experience of the Chief Information Manager and should he not be available, there may be a key dependency risk.	Med	We recommend that where possible, staff are 'multi skilled' to ensure continuity of service and/or applications support, so that should key IT support staff be unavailable for any reason, there is minimal, to negligible impact on operational activities - a staff skills needs assessment should be performed with an action plan devised. It is also recommended that, in line with current management thinking, procedure guidance is compiled for all core activities undertaken within IT.

MANAGEMENT RESPONSE	RESPONSIBILITY AND IMPLEMENTATION DATE
A skills matrix (that you have already seen) is maintained highlighting the skill levels of all staff across the Operations and Application teams. The training plans will be further deployed to address gaps as well as develop the individual team members. This is further picked up in appraisals and embedded in personal development plans.	***Responsible Officer:*** ***Chief Technology and Information Manager*** ***Implementation Date: July 2016***

DETAILED RECOMMENDATIONS

RISK: Unauthorised access to systems is obtained impacting the integrity of data held

Ref.	Finding	Sig.	Recommendation
3	It was identified that the practices undertaken around user access management are inconsistent across Active Directory (AD) and individual applications and that there is limited guidance or process notes to act as a 'directive' control. The processes are: **Active Directory (AD):** AD is managed by the IT team. For new starters, the support staff will create a new AC account once a request has been received by the line manager of the starter. However, we were informed that the time frames in which these requests are received is inconsistent and on occasions they are not received until after the employee has started, resulting in tight requirements to ensure that it does not impact on operational activity. For leavers, we were informed that requests are sporadic and often not received until some time after an employee has left. **In-scope Applications:** For individual applications, in terms of application access controls, this is performed by local administrators. We were informed that there are some documents 'scattered' in different locations; however, they are out of date. In the main, the process requires a line manager to notify of a new starter and detail the role that the member of staff is to undertake. It was identified through discussion that the process can differ dependent on the person that is setting up access; however, a common theme through interviews was that when a request is received, an account of another user is 'mirrored' which means that the new user will get the same credentials as the copied account. *(Continued on next page)*	Med	We recommend that the user access management process (to include, new starters, internal moves and leavers) is reviewed and guidance is produced to act as a directive control and promote consistency across the different applications. This should be distributed to relevant stakeholders to enhance the consistency of application. Where applicable, this should be linked with a HR starters and leavers process to enhance the time frame of requests.

DETAILED RECOMMENDATIONS

RISK: Unauthorised access to systems is obtained impacting the integrity of data held			
Ref.	**Finding**	**Sig.**	**Recommendation**
3	*(Continued)* Although this process may be more efficient, some users access rights can be enhanced organically which, when copied, presents a risk that a new user may be granted more access than is required for their role. It should be noted that we were unable to perform any sample testing of user access levels in order to quantify any associated risk. This information was requested from the outset of the review however, the data was considered too large to provide and therefore we have to conclude without receiving the data.	Med	

MANAGEMENT RESPONSE	RESPONSIBILITY AND IMPLEMENTATION DATE
There is already manual process to link up the work required by HR and ICT. However, the scope for automation has already been identified, and is scheduled on the ICT work plan for review and amendment by mid July 2016. This will include automated, early notification of new starters and leavers as soon as this information is updated on the HR system (iTrent). This will allow ICT to proactively contact managers and initiate the processes to provision new equipment / services for new starters and to close down access and recover assets for leavers.	***Responsible Officer:*** ***Chief Technology and Information Manager*** ***Implementation Date: July 2016***

DETAILED RECOMMENDATIONS

RISK: When authorised administrator access to systems is utilised, data is manipulated or compromised other than to test, monitor and upgrade systems as expected

Ref.	Finding	Sig.	Recommendation
4	There are a number of staff with privileged user access rights within the Council and although records indicate that this level of access is required for an aspect of their roles, there is no system audit trail activated in order to provide a mechanism of tracing whether inappropriate action has been taken. This increases the risk that either malicious or accidental changes could be made without any identifiable accountability.	Med	We recommend that management switch on the system audit trails to ensure that, in the event of an incident, they are able to trace the full history or events. To ensure control over those with such elevated access they can delete audit trails, where practicable, either a block of this access should be introduced or alternatively, a script should be developed to alert for any alteration of the audit trail.

MANAGEMENT RESPONSE	RESPONSIBILITY AND IMPLEMENTATION DATE
Network Access level logging is already in place as part of the existing PSN compliance. We will review the availability and feasibility of implementing application level logging for the key applications (PARIS, Academy, Northgate Housing, Agresso) by end of August 2016	***Responsible Officer:*** ***ICT Operations Manager*** ***Implementation Date: August 2016***

DETAILED RECOMMENDATIONS

RISK: Council applications do not integrate correctly with interfacing applications resulting in lost or inaccurate data			
Ref.	**Finding**	**Sig.**	**Recommendation**
5	The IT applications support staff who have responsibility for the technical aspects of the interfaces for in-scope applications have developed scripts that will highlight when an interface has not run as designed or failed in its entirety. Although these scripts are effective in their output, they are not all automated which means there is a reliance on support staff to ensure that they perform their daily routine. If they are not around, for example, on leave or off sick, the responsibility would fall on another member of staff. This presents a risk that, if not done, there is a delay in the identification of issues and mitigating actions for failed interfaces.	Med	We recommend that the current scripts are enhanced to enable automated alerts to be generated in the event of issues with interface failures. This alert should go to a managed central mailbox rather than to an individual.

MANAGEMENT RESPONSE	RESPONSIBILITY AND IMPLEMENTATION DATE
A new application level monitoring solution (Nagios) is being implemented in June 2016. This will provide a central location for application and network level monitoring and alerts including interfaces. Interface alerts will be in place by end of August 2016.	*Responsible Officer:* *Application Manager* *Implementation Date:* *August 2016*

OBSERVATIONS

PCI DSS

The PCI DSS self-assessment for the Council will be completed by end of August 2016 and will form part of the re-procurement of the payment systems scheduled to be in place by end of December 2016. Internal Audit will be reviewing PCI DSS in 2016-17.

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
Paul Fleming	Chief Technology and Information Manager
Paolo Coraci	Senior IT Support Analyst (PARIS)
Phil Dean	Senior Application Specialist (Academy, ePay)
Matt Lapworth	Senior Application Specialist (Northgate Housing)
Stacie Tomkins	Agresso Specialist
Simon Park	Officer
Paul Collins	Officer
Nikki Pearce	Procurement Officer
Lauren Armstrong	Housing Officer
Caroline Wood	Procurement Officer
Pauline Hull	Income/Agresso Officer

APPENDIX II - DEFINITIONS

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

Oxford City Council (the ‘Council’) utilise many IT applications to support the delivery of their objectives. These applications and the data held on them must be held securely to minimise manipulation of data, interface with each other to support successful transfer of information and be upgraded/testing to ensure they are fit for purpose.

The responsibility for this areas falls under the Head of Business Improvement and managed on a day-to-day basis by the Chief Technology Manager. The Council utilise many applications such as Agresso (General Ledger), Paris (Income), Northgate (Housing), Academy (Benefits) and a Customer Support Application. For each application there are officers who have oversight of the application and would report to the Chief Technology Manager should concerns arise with the applications operation.

These systems all have significant numbers of transactions which run through them daily which are all accessed by a vast and varied number of staff, are subject to upgrades and testing and have specific access controls. This review will assess the control environment to support the objectives to safeguard these applications from inappropriate use and manipulation of data.

PURPOSE OF REVIEW

To review the design and effectiveness of controls in relation to applications to provide assurance over the accuracy, completeness and timeliness of transactions undertaken.

SCOPE OF REVIEW

The scope is as per the Key Risks identified overleaf.

EXCLUSIONS

We will only be performing a high level review of Payment Card Industry (PCI) compliance as this is primarily an application review.

APPENDIX III – TERMS OF REFERENCE

APPROACH

Obtain an understanding of the risk and controls with regards to Council applications through discussions with key personnel, review of systems documentation and substantive tests. Our approach includes:

- Identifying the key risks
- Evaluating the design of the controls in place to address the key risks
- Testing the operating effectiveness of the key controls.

KEY RISKS

Based on the risk assessment carried out during the creation of the internal audit operational plan, our discussions with management, and our collective audit knowledge and understanding, the key risks associated with the area under review are:

- Inadequate systems knowledge and training for those who manage interfaces to ensure data is properly secured and managed
- Unauthorised access to systems is obtained impacting the integrity of data held
- When authorised administrator access to systems is utilised, data is manipulated or compromised other than to test, monitor and upgrade systems as expected
- Council applications do not integrate correctly with interfacing applications resulting in lost or inaccurate data
- When the cases are subject to a ‘near-miss events’ for applications held, lessons are not captured and learned to support continuous learning
- High level controls are inadequate to ensure compliance with Payment Card Industry (PCI) requirements.

DOCUMENT REQUEST

Where available, please ensure that electronic copies of the following documents have been forwarded to us in advance of the review:

- Listing of all unauthorised access from 1 April 2015 to date
- Listing of all data lost/manipulated from 1 April 2015 to date
- Structure showing all applications the Council’s holds and how they interface with each other
- List of training provided to Business Improvement and Technology Officers from 1 April 2015 to date
- Latest IT risk register
- Any Process documents relating to applications in use.

These documents will assist the timely completion of our fieldwork, however this list does not necessarily constitute a complete list of all documentation and evidence that we may need as part of our review.

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.

www.bdo.co.uk