AGENDA ITEM: 10 Page nos. 34 - 46

Meeting	Audit Committee
Date	27 April 2009
Subject	**External Audit Report on IT Controls**
Report of	Director of Resources
Summary	To consider the report from the external auditor on IT Controls.

Officer Contributors	Kylton Trim, Head of Information Systems
Status (public or exempt)	Public
Wards affected	Not applicable
Enclosures	Appendix A – IT Controls Report (November 2008)
For decision by	Audit Committee
Function of	Council
Reason for urgency / exemption from call-in (if appropriate)	None

Contact for further information: Kylton Trim, Head of Information Systems 020 8359 7905

1. RECOMMENDATIONS

1.1 That the matters raised by the external auditor relating to IT Controls be noted.

1.2 That the officer response to the matters raised by the external auditors be noted.

1.3 That the Committee consider whether there are any areas on which they require additional information or action.

2. RELEVANT PREVIOUS DECISIONS

2.1 None

3. CORPORATE PRIORITIES AND POLICY CONSIDERATIONS

3.1 Effective and efficient IT controls will contribute to the corporate priority More Choice Better Value, by ensuring that IT plans are aligned with the objectives of the Corporate Plan, and that systems are sufficiently protected.

4. RISK MANAGEMENT ISSUES

4.1 Failure to have a robust set of IT controls place the confidentiality, security and integrity of the Council's data at risk.

5. EQUALITIES AND DIVERSITY ISSUES

5.1 None

6. USE OF RESOURCES IMPLICATIONS (Finance, Procurement, Performance & Value for Money, Staffing, IT, Property, Sustainability)

6.1 The Council's information systems are governed by a number of IT controls designed to protect the integrity, confidentiality and availability of the data held within systems. Effective IT controls enable compliance with Data Protection legislation and contribute to efficient IT services that represent value for money by ensuring the alignment of IT plans with corporate objectives. [Suggest that each of these resources may need to be addressed separately]

6.2 There are no specific staffing, financial or property implications.

7. LEGAL ISSUES

7.1 None arise as a result of the contents and recommendations of this report

8. CONSTITUTIONAL POWERS

8.1 Part 3, Section 2 of the Constitution: the terms of reference for Audit Committee includes consideration of the external auditor's annual letter, relevant reports, and the report to those charged with governance.

9 BACKGROUND INFORMATION

9.1 The Council's external auditor, Grant Thornton, has found that in general the controls over Information Technology are adequately designed. Recommendations for improvements have been made in the area of strategy, business continuity and Information Technology policies.

9.2 The Council is in the process of refreshing the Information Systems strategy. The external audit report has recommended the formation of a steering group to ensure the alignment of the strategy with corporate objectives. An Information Systems strategy group will be formed by April 2009.

9.3 The external auditor recommended that Information Systems policies are reviewed and that a web-based master document be created with links to individual policies. In addition, that the policies and procedures should be reissued to all users of information systems. This will be complete by April 2009.

9.4 The recommendation that management should consider the creation of an IT Business Continuity Plan aligned to the needs of the business is agreed. Draft IT recovery plans are in place and will be agreed with the business through existing business continuity channels.

9.5 A recommendation to review the external audit report of third party suppliers has been agreed, this will be complete by April 2009.

9.6 The recommendation to review the Council's Active Directory and SAP system is agreed and arrangements have been made with the Council's Internal Audit section.

10. LIST OF BACKGROUND PAPERS

10.1 None

Legal:
CFO:

London Borough of Barnet

Report on Information Technology Controls

November 2008

Contents **Page**

1 Executive summary 1

2 Purpose and scope 3

3 Recommendations 4

Appendix

A Action Plan

1 Executive summary

1.1 Introduction

This review provides an independent assessment of the effectiveness of the design of London Borough of Barnet's controls over Information Technology. This report is intended primarily for use by the Council in developing the organisation's information provision in the future.

The review was conducted as part of our normal audit planning procedures, to arrive at an assessment of the risk that controls fail to prevent error or fraud. This assessment is designed to establish the feasibility of placing reliance on internal controls and thereby potentially reducing the overall level of substantive testing we need to perform in order to reach our opinion on the truth and fairness of the Council's Annual Financial Statements. It also feeds into our overall conclusions in respect of the auditor's local evaluation and our value for money conclusion.

1.2 Conclusions

Overall, General Controls over Information Technology are adequately designed, apart from the following areas for improvement. References in brackets are to the detailed findings and recommendations in section 3 of this report. The High Priority issues are

- The need for the Information Management and Technology Board to review and approve the implementation of the Council's Information Systems Strategy.

- Create a single web-based "master document" to cover all IT security and administration, structured to contain appendices, where material can be split between different staff and where staff can sign to indicate that they understand their role and responsibility in respect of the Council's secure systems and data.

- There are IT Disaster Recovery plans in place, but these plans are not designed to meet the wider business's needs in the event of an incident. Management should consider the creation of an IT Business Continuity Plan (BCP) which is aligned to the needs of the business, taking into account the different business needs and IT systems requirements for specific monthly events e.g. payroll, and annual events like the production of Annual accounts and Government returns.

- Under the auspices of the Modernised Ways of Working (MWW) programme review we completed a detailed security review of the Council's current and proposed security environment. We found that there were gaps in security planning and identified a need for a council wide master document covering all IT security aspects. One key issue was that we were unable to establish the level of review and monitoring of operating systems and security logs. Regular audits of server systems and security event logs are required to establish that secure access to enterprise data is maintained. Security policies and procedures should be established and communicated to all users of IT across the Council prior to the release of Employee and Manager Self Service Modules.

The other issues identified from our work are as follows:

- Server backup policies and procedures, undertaken by third parties such as Logica should be confirmed and communicated to relevant individuals so that business resumption plans can be effective as and when required.

- Regular Active Directory and SAP user reviews may be of benefit to the Council at this time of major IT change in data access and delivery.

Our recommendations, contained in the body of this report, are designed to address these issues.

1.3 Responsibility of the IT Management

These key issues were previously discussed with Kylton Trim, Head of Information Systems and Rick Sweeney, Head of Infrastructure and Operations, earlier this year and have been agreed with Kylton Trim and Shahin Farjami, Assistant Director for Shared Services on November 2008.

We would point out that the matters dealt with in this report came to our attention during the conduct of our normal audit procedures which are designed primarily for the purpose of expressing our opinion on the financial statements of the Council.

In consequence, our work did not encompass a detailed review of all aspects of the system and controls and cannot be relied upon necessarily to disclose defalcations or other irregularities, or to include all possible improvements in internal control that a more extensive special examination might develop.

We would be pleased to discuss any further work in this regard with the Council.

1.4 Confidentiality

This report is strictly confidential and although it has been made available to management to facilitate discussions, it may not be taken as altering our responsibilities to the Council arising under the Audit Commission's Code of Audit Practice and the Statement of Responsibilities.

The contents of this memorandum should not be disclosed to third parties without our prior written consent.

2 Purpose and scope

2.1 The purpose of this report

The purpose of this report is to highlight the key issues arising from our IT audit work, performed in preparation for the audit of the financial statements of the Council for the year ended 31 March 2008.

The document is also used to report to management to meet the mandatory requirements of International Standard on Auditing (UK & Ireland) (ISAUK) 260.

2.2 The scope of our review

The review covered the Information Systems used by the Council to manage its business, covering the general controls over all systems, both financial and administrative.

2.3 Objectives

The objective of the review was to assess the adequacy of the design of the Council's General Controls over Information Systems under the following headings:

- Management and Organisation
    - develop and implement plans
    - identify and asses risks
    - operate reliable systems
    - hire and retain people
    - manage third-party services
- Applications
    - acquire and maintain operating and database systems
    - acquire and maintain applications
- Security
    - administer policies and procedures
    - protect data and enforce segregation of duties
    - limit external access to systems
    - protect physical assets.

3 Recommendations

In the following recommendations, High Priority recommendations correspond to fundamental control risks; Medium Priority recommendations apply to control risks that exist but are not considered fundamental; Low Priority recommendations are designed to assist in the achievement of best practice.

3.1	**Recommendation: The Information Management and Technology Board should review and approve the implementation of the Council's Information Systems Strategy.**
High Priority	It was noted that the IT strategy was currently being updated and was in draft. Initially we were unable to obtain an up to date Information Systems Strategy. The roles of IT strategic leads are now under the management of the Head of IS and this implementation is expected to proceed.

3.2	**Recommendation: Create a single web-based "master document" with links to other documents covering all IT security and administration, structured to contain appendices, where material can be split between different staff and where staff can sign to indicate that they understand their role and responsibility to LBB secure systems and data.**
High Priority	As an integral part of the review of the MWW project we conducted a detailed security review of policies and procedures. We found gaps in security policies. Procedures were weak and we agreed with the Head of IS and the MWW Programme Manager that a council wide master document covering all IT security aspects was necessary.

3.3	**Recommendation: Management should consider the creation of an IT Business Continuity Plan (BCP) which is aligned to the needs of the business.**
High Priority	There are IT DR plans in place. However these plans need to be incorporated into an IT BCP which is aligned to the needs of the business, taking into account the different business needs and IT systems requirements at specific monthly events e.g. payroll, and annual events like the production of Annual accounts, Government returns etc.

3.4	**Recommendation: Security policies and procedures should be established and communicated to all users of IT across the Council prior to the release of Employee and Manager Self Service (ESS and MSS) modules on SAP HR**
High Priority	While some Security Policies and Procedures exist, our work indicated that there were weaknesses. Processes were being put in place to ensure that stronger security controls were implemented across the Council. This was considered for a number of areas. • MWW roll out would result in the deployment of a number portable devices e.g. PCs and Tablets the security of data held on these devices varied across the Council. • The SAP HR development and trials highlighted the need for all staff to acknowledge the revised security polices and procedures required for accessing highly personal sensitive data, which will become accessible at the desktop. Whilst there was no evidence provided of existing data security breaches there were limited processes in place to deal with such matters at the highest level of severity. Specifically, although procedures exist for adding new users and removing former employees' access to the systems, the policy for removing leavers from systems was not found to be operating effectively. Controls do not exist to ensure that former employees are removed from the systems on a timely basis. The release of SAP HR (ESS and MSS) will also serve to support joiner and leaver polices going forward.

3.5	**Recommendation: Server backup policies and procedures, undertaken by third parties e.g. Logica and other Third part suppliers should be confirmed and communicated to relevant individuals in IT to ensure business resumption plans can be effective and available as and when required.**
Medium Priority	There are third party suppliers who have procedures in place for the back up and restoration of data and systems. However the Head of IS and Head of IT and Operations were not aware of a current audit report from Logica which would confirm the status and levels of control around back ups and operating systems access security and control. We are aware that the concepts of e-volt are being discussed and shared data centres with other Local Authorities are being considered., including plans to automate all of the Council servers and systems backups in the future. There is a risk that the details of systems and their last back up processes can not be utilised effectively in the event of as incident for IT BCP and business resumption purposes.

3.6	**Recommendation: Regular Active Directory and SAP user reviews may be of benefit to the Council at this time of major IT change in data access and delivery**
Medium Priority	Regular Active Directory and SAP user access controls and security reviews should take place with the number of Council developments taking place e.g. MWW, HR ESS and MSS. The Council should consider a full independent review of Active Directory. Reviews of key applications like SAP should be performed on a regular basis. This could be done by Internal Audit. .

A Action Plan

Ref	Recommendation	Priority	Management Response	Responsible Officer	Action Date
3.1	The Information Management and Technology Board should review and approve the implementation of the Council's Information Systems Strategy.	High	Agreed	Head of IS	1 April 2009
3.2	Create a single web-based "master document" with links to other documents covering all IT security and administration, structured to contain appendices, where material can be split between different staff and where staff can sign to indicate that they understand their role and responsibility to LBB secure systems and data.	High	Agreed	Head of IS	1 April 2009
3.3	Management should consider the creation of an IT Business Continuity Plan (BCP) which is aligned to the needs of the business.	High	Draft plans are in place for all aspects of IT. We are in the process of updating corporate BCPs, which are being peer challenged by the Business Continuity Board. The plans have been agreed in principle but we need the business to have plans in place so that IT can fit in. The paper will go to the Councillors Group in January 2009 and final plans will be in place by 1 April 2009	Head of IS	1 April 2009
3.4	Security Policies and Procedures should be reissued to all users of Information Systems, along with training in the importance of information security. .	High	A reminder is to be sent out to all users setting out the key principles governing such issues as choice of passwords, use of passwords, the importance of locking PCs etc This will go in the First Team Bulletin.	Head of IS	1 April 2009
3.5	Server backup policies and procedures, undertaken by third parties e.g. Logica and other Third party suppliers should be confirmed and communicated to relevant individuals to ensure business resumption plans can be effective as and when required	Med	Agreed	Head of IS	1 April 2009

Ref	Recommendation	Priority	Management Response	Responsible Officer	Action Date
3.6	In view of the number of developments taking place, regular Active Directory and SAP user access controls and security reviews should take place .The Council should consider a full independent review of Active Directory and key applications like SAP, which should be performed on a regular basis. This could be done by Internal Audit	Med	Agreed. Arrangements will be made with Internal Audit for regular reviews of access controls to take place	Head of IS	1 April 2009