London Borough of Haringey

Report on Information Technology Controls

July 2009

Contents **Page**

Appendix

1 Executive summary

1.1 Introduction

This review provides an independent assessment of the effectiveness of the design of the London Borough of Haringey's ('the Council's) general controls over information technology in areas that may impact on the financial statements. This report is intended primarily for use by the Council in developing its control framework over information technology 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 material error or fraud. This assessment is designed to establish the feasibility of placing reliance on internal controls to reach our opinion on the truth and fairness of the Council's Annual Financial Statements.

1.2 Conclusions

Overall, we have concluded that, in the areas examined, the risk management activities and controls are suitably designed. There are no significant findings arising from the audit. However, we have highlighted a small number of points for consideration by management that seek to enhance existing controls. These can be found at section three with an action plan to record management's response.

1.3 Responsibility of Management

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.

Our work did not encompass a detailed review of all aspects of the system and controls, nor have we included all possible improvements in internal control that a more extensive examination might develop. However, we would be pleased to discuss any further work in this regard with the Council.

1.4 Use of this report

This report has been prepared solely for use by the Council and should not be used for any other purpose. We assume no responsibility to any other person.

1.5 Acknowledgments

We would like to record our appreciation for the positive co-operation and assistance provided to us by the IT department and other staff at the Council during the course of our audit.

Grant Thornton UK LLP

July 2009

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 London Borough of Haringey for the year ended 31 March 2009.

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 both administrative and operation controls over the Network and SAP application. The Human Resources, Payroll, Finance and Training and Events modules are currently deployed within SAP.

Other applications utilised by the Council include:

- I-Plan, I-Build, I-Gaz: property management system
- Framework-I: Children and Young people Services system
- OHMS: Housing Management system
- RadiusICON: Cash receipting system

We have not sought to review controls over these or other applications.

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:

- Security Administration
    - establish effective security environment
    - manage internal user access
    - manage remote and third-party access
    - monitor access to IT systems
- Program Maintenance
    - establish effective maintenance environment
    - initiate change requests
    - design, develop and configure program changes
    - promote changes to production

- Program Execution
    - establish effective program execution environment
    - schedule batch programs
    - execute authorised programs
    - monitor execution of programs
- New System Implementation
    - establish effective new system implementation environment
    - initiate new system project
    - define system requirements and specifications
    - design, develop, configure and integrate system
    - implement and deploy system

3 Recommendations

All recommendations listed in the following table are of **low** priority and are designed to assist in the achievement of best practice.

3.1 Acknowledgement of Acceptable Use Policy by users
The PCI Gap Analysis report states that staff are not required to acknowledge in writing acceptance of the security policy and procedures. Upon inquiry, we found that this was per HR's advice. Management should review the existing procedures for policy acknowledgements with a view to introducing a process whereby all existing and new staff are required to acknowledge, in writing, their understanding of the security policy and procedures.

3.2 SAP password complexity
There are currently no controls in place within SAP to prevent the use of common/predictable passwords. However, management is considering utilising the single sign-on facility for access to SAP. Alternatively, we recommend that the table containing common passwords prohibited from use (Table USR40), should be populated and updated on a regular basis. This would help in maintaining active password controls and limit the risk of unauthorised access into SAP.

A Action Plan

Ref	Recommendation	Priority	Management Response	Responsible Officer	Action Date
3.1	Management should review the existing procedures for policy acknowledgements with a view to introducing a process whereby all existing and new staff are required to acknowledge, in writing, their understanding of the security policy and procedures.	Low	All employees(that have received a new or amended contract) are required to sign a copy which has as an appendix including the T&C letter which by its wording includes reference to all policies and procedures (inc security). Management do not consider a separate signing of this policy & procedure is therefore required. The wording in the recent PCI Gap Analysis Audit could have been more helpful in this instance.	Ian Andrews	None Required

Ref	Recommendation	Priority	Management Response	Responsible Officer	Action Date
3.2	Management should review the SAP password settings and ensure that appropriate complexity settings are enabled, where possible utilising the single sign-on facility. Alternatively, we recommend that the table containing common passwords prohibited from use (Table USR40), should be populated and updated on a regular basis. This would help in maintaining active password control and limit the risk of unauthorised access into SAP.	Low	The long term solution is one of single sign on which is planned to be discussed as part of the forthcoming IT strategy roadmap. In the short term a review of access to all SAP systems is being undertaken by SAP FST including existing password controls and as part of this review table USR40 will be populated. This review will be in line with current IT network password controls.	Ian Andrews	December 2009