Havering
LONDON BOROUGH

AUDIT COMMITTEE
25 June 2013

Subject Heading:	Internal Audit Interim Progress Report
Report Author and contact details:	Vanessa Bateman – Internal Audit & Corporate Risk Manager ext 3733
Policy context:	To inform the Committee of the outcomes of the remaining 2012/13 audits.
Financial summary:	N/a

The subject matter of this report deals with the following Council Objectives

Clean, safe and green borough	X
Excellence in education and learning	X
Opportunities for all through economic, social and cultural activity	X
Value and enhance the life of every individual	X
High customer satisfaction and a stable council tax	X

SUMMARY

This is an interim report to advise the Committee on the final 2012/13 audit plan reports issued since the last meeting.

RECOMMENDATIONS

---

1. To note the contents of the report.

2. To raise any issues of concern and ask specific questions of officers where required.

REPORT DETAIL

This progress report contains an interim update to the Committee regarding Internal Audit activity presented in four sections.

Section 1   Final Reports issued after 31st March 2013.

A summary of the work undertaken in quarter four, for which the final report was issued after the 31st March 2013, is included in this section of the report.

Section 2   Management Summaries

Summaries of all final reports issued.

Section 3   Schools Audit Work

A summary of schools final reports issued.

Section 4   Outstanding Audit Recommendations

The details regarding status, as at the end of May, of all outstanding recommendations are included within tables for information.

IMPLICATIONS AND RISKS

Financial implications and risks:

Failure to either implement at all or meet the target date may have control implications, although these would be highlighted by any subsequent audit work.   There are no financial implications or risks arising directly from this report.

Legal implications and risks:

None arising directly from this report

Human Resources implications and risks:

None arising directly from this report

Equalities implications and risks:

None arising directly from this report

BACKGROUND PAPERS

None.

Section 1   Audit Work finalised after 31st March.

1.1   Schedule 1 details the work completed in quarter four for which final reports were issued after the 31st March 2013. Details are listed in the table below and management summaries under Section 3 starting on the next page.

1.2   Reviews have also been undertaken on Information Governance – Service Area Control and Compliance and Provider Compliance.

1.3   A review was also undertaken on ISS Performance Management to support work by Management in this area.

SCHEDULE 1: 2012/2013 – Systems Audits Completed

Report	Opinion	Recommendations				Ref Below
		High	Med	Low	Total	
Debt Management	Substantial	0	1	0	1	**2** (1)
Council Tax	Substantial	0	3	2	5	**2** (2)
Housing Benefits	Substantial	0	0	0	0	**2** (3)
Budgetary Control incl. CP	Substantial	0	1	0	1	**2** (4)
Accounts Payable	Substantial	0	1	0	1	**2** (5)
Accounts Receivable	Substantial	0	2	1	3	**2** (6)
Modern Governance	Substantial	3	7	2	12	**2** (7)
Release of Software	Limited	3	0	0	3	**2** (8)
Operating Systems	Limited	4	2	0	6	**2** (9)
Contracts & Procurement	Substantial	0	1	0	1	**2** (10)

Section 2   Management Summaries

Debt Management	Ref 2 (1)

2.1   Background

2.1.1   The council has multiple services that generate an income. Many of these services are supplied before a payment is received, therefore creating a debt to the council. A list of the areas where debts are incurred, as identified during the audit, is attached as Appendix 1 of this report.

2.1.2   The Constitution outlines responsibilities with regards income collection.

2.1.3   The Council has a Corporate Debt Management Policy.

2.1.4   Levels of debt within the organisation are overseen by The Debt Management Board (DMB) chaired by Head of Customer Services.

2.1.5   In February 2013 a Senior Management restructure was launched part of this proposal is to bring all debt recovery activity into Finance/new Resources Directorate.

2.1.6   Summary of Audit Findings

2.1.7   The Corporate Debt Management Policy is being used as a guideline when invoicing and recovering debts. However it has been some time since the Corporate Debt Management Policy has been reviewed and updated.

2.1.8   Based on the work we have completed approximately 15 officers work across the organisation on income and debt recovery.

2.1.9   In the past four years the Group Director Resources has not been asked to approve any procedures within service area as required by the constitution.

2.1.10 Debt Management Board meetings showed a trend of debts generally being reduced.

2.1.11 It is noted that some services follow procedures that differ from the corporate policy.

2.1.12 Audit Opinion

2.1.13 As a result of this audit one medium priority recommendation relating to:
- Communicating potential points for consideration / action when implementing the planned new arrangements.

2.1.14 **Substantial Assurance** has been given as while there is a basically sound system, there are limitations that may put some of the systems objectives at risk, and/or there is evidence that the level of non-compliance with some of the controls may put some of the system objectives at risk.

2.2   Background

2.2.1   Historically the provision of the Council Tax service was delivered by one dedicated team. In 2011 the administration of Council Tax was split into two main areas. Processing and administration of Council Tax is dealt with by the Contact Centre based at Mercury House who provides the customer facing element of the service. Back office functions have been retained by a team located at the Town Hall.

2.2.2   Summary of Audit Findings

2.2.3   Management information is not currently available from the Information @ Work system and so is being collated manually. Business Systems are working on producing a report to resolve this issue. No recommendation has been raised.

2.2.4   Instances of work that had already been processed were found within the Contact Centre in-tray. No recommendation is being raised as some feedback will be gathered to identify the scale of the issue.

2.2.5   Information relating to planning applications / completions for property extensions has not been reported to the Valuation Office since October 2011, changes in property bands may therefore not be being identified. Whilst this is not the responsibility of this team, there is a possible future impact on the services revenue.

2.2.6   Four accounts on the Academy system are not being billed for Council Tax, as a liable party has not been determined. Planning are conducting a review of the properties / accommodation located on this site. Council Tax will take appropriate action based on the results of this work. No recommendation has been raised.

2.2.7   There are discrepancies between the property numbers and bandings information held by the Valuation Office compared to the Academy system. These discrepancies are factored into reconciliations. No recommendation has been raised.

2.2.8   Clear roles, responsibilities and timescales for taking action on Data Tank and NFI issues have not been established.

2.2.9   Write offs are not being consistently processed in line with the procedure.

2.2.10 A local document retention policy for both hard copy and electronic data is not in place.

2.2.11 Staff that have left the Council still have access rights to the system. Reviews of users have not been happening, although a report is in the process of being generated for this to be completed. No recommendation has been made as this is already being resolved.

2.2.12 Declarations signed by staff to support notification of actions not permitted on the Academy system have not been extended to cover all users of the system.

2.2.13 Audit Opinion

2.2.14 As a result of this audit three medium and two low priority recommendations have been raised relating to the need for:
- Clarification over responsibilities for passing information to the Valuation Office; *(Medium Priority)*
- Clear roles and responsibilities for processing Data Tank / NFI changes on the system in a timely manner; *(Medium Priority)*
- Documentary evidence to support the write off and approval; *(Medium Priority)*
- A local document retention policy to be produced; *(Low Priority)* and
- Declaration forms for accessing Academy to be expanded to include all non-read only users outside of the Council Tax and Contact Centre teams to be completed. *(Low Priority)*

2.2.15 **Substantial Assurance** has been given as while there is a basically sound system, there are limitations that may put some of the systems objectives at risk, and/or there is evidence that the level of non-compliance with some of the controls may put some of the system objectives at risk.

2.3 Background

2.3.1 In February 2013, a risk based approach to the assessment of housing benefit claims was adopted by the Council. Instead of a blanket approach for assessing all claims in the same way, Risk Based Verification (RBV) allows the level of checks undertaken to be determined by the level of risk that the claim poses.

2.3.2 The Council are using the Capita Risk and Verification Portal to assess claims.

2.3.3 **Summary of Audit Findings**

2.3.4 Limited resources are available to carry out the manual elements of the recovery process, causing a backlog in recovery. This issue has already been included in the Revenues & Benefits Action Plan to be reviewed in May 2013, so no recommendation has been raised.

2.3.5 Minor issues with the data upload from NatWest have resulted in presented cheques appearing on the unpresented cheques report. Due to the small number of claims being paid by cheque as well as regular monitoring and reconciliation of these cheques, no recommendation is being raised.

2.3.6 A local document retention policy is not in place. The same issue was highlighted as part of the Council Tax audit and recommendations made to resolve these issues. No additional recommendations have therefore been raised within this report.

2.3.7 Staff that have left the Council still have access rights to the system. The same issue was highlighted as part of the Council Tax audit and recommendations made to resolve these issues. No additional recommendations have therefore been raised within this report.

2.3.8 Declarations signed by staff to support notification of actions not permitted on the Academy system have not been extended to cover all users of the system. This issue has also been raised as part of the Council Tax report and so no recommendations have been raised.

2.3.9 **Audit Opinion**

2.3.10 As a result of this audit no recommendations have been raised.

2.3.11 **Substantial Assurance** has been given as while there is a basically sound system, there are limitations that may put some of the systems objectives at risk, and/or there is evidence that the level of non-compliance with some of the controls may put some of the system objectives at risk.

| **Budgetary Control incl. CP** | **Ref 2 (4)** |

2.4   Background

2.4.1   Budget monitoring is the responsibility of Cost Centre Managers (CCMs). An online forecasting system called CP (Collaborative Planning) was introduced in June 2012. This system has replaced the previous reliance on excel spread sheets to record and report monthly forecasts.

2.4.2   The CP system interacts with the Oracle Financials system to provide an integrated financial management solution.

2.4.3   **Summary of Audit Findings**

2.4.4   The introduction of new technologies in this process has strengthened the Council's budget monitoring and forecasting processes by ensuring that more timely data is available to CCMs. However, the process is still reliant on accurate forecasting by CCM's regarding activity in their service area and the Head of Service and Finance providing critical control mechanisms to detect, report and resolve inaccuracies and instances on non-compliance.

2.4.5   During 2012/13 instances of non-compliance have been identified and a report with recommendations presented to Corporate Management Team by Finance. This focus on compliance and ensuring efficient controls are operating is not a new challenge to the Council but one that is even more significant with the culture change towards self-service. As a result, some of the findings in this audit will be mitigated by the proposed recommendations in the CMT report, so no recommendations have been raised in these instances.

2.4.6   Management information available to identify instances of non-compliance is available, but is not currently being utilised, impacting on Operational Finance's resources.

2.4.7   **Audit Opinion**

2.4.8   As a result of this audit one medium priority recommendations relating to the need for the Completion status report to be utilised to monitor non-compliance.

2.4.9   **Substantial Assurance** has been given as while there is a basically sound system, there are limitations that may put some of the systems objectives at risk, and/or there is evidence that the level of non-compliance with some of the controls may put some of the system objectives at risk.

2.5 Background

2.5.1 The Accounts Payable (AP) function became part of Internal Shared Services as part of the initial implementation of ISS in April 2011.

2.5.2 A Control Working Group was carried out for Accounts Payable for 11/12 that highlighted specific risk areas and potential solutions. One previous highlighted issue not yet fully resolved has been reiterated within this report.

2.5.3 Creditor payments through the Councils bank account for 2011/12 were a little over £420 million. Creditor payments as at 20/3/13 were a little under £345 million.

2.5.4 During 2012/13 the number of invoices being paid via the AP function has reduced due to the implementation of the IProcurment system. 21443 invoices were paid in the final three months of 2012/13, compared to 23727 in the previous three months.

2.5.5 The AP system is part of the One Oracle Project so the system will be upgraded to version 12 in November 2013.

2.5.6 Summary of Audit Findings

2.5.7 Financial Framework/ Procedures were last updated before introduction of Internal Shared Services. It is noted that all policy and procedural updates are now part of the One Oracle Project and will not be completed in advance.

2.5.8 Authorised signatories are not currently completed. Checks are carried out on payments over £50k

2.5.9 Supplier list contains multiple duplicates.

2.5.10 Audit Opinion

2.5.11 As a result of this audit one medium priority recommendation relating to:
- Financial Framework to be updated to include ISS processes.

2.5.12 **Substantial Assurance** has been given as while there is a basically sound system, there are limitations that may put some of the systems objectives at risk, and/or there is evidence that the level of non-compliance with some of the controls may put some of the system objectives at risk.

2.6 Background

2.6.1 The Accounts Receivable (AR) function became part of Internal Shared Services as part of the initial implementation of ISS in April 2011.

2.6.2 A Control Working Group was carried out for AR for 11/12 that highlighted specific risk areas and potential solutions. Previous highlighted issues not yet resolved have been reiterated within this report.

2.6.3 The AR system is part of the One Oracle Project so the system will be upgraded to version 12 in November 2013. It should also be noted that a decision has been made to implement a corporate debt recovery team within the Resources Directorate which may also impact on the system going forward.

2.6.4 A total of 12,305 invoices have been raised by the Accounts Receivable team between April and September 2012, compared to 11,766 during the same period in 2011.

2.6.5 In September 2011 arrears totalled £7,724,810 compared to £5,663,016 at September 2012

2.6.6 **Summary of Audit Findings**

2.6.7 Procedures are not being updated when changes are made.

2.6.8 Declarations of Interest are not being completed by members of the Accounts Receivable Team.

2.6.9 Data Protection & money laundering training is not undertaken & procedures documented.

2.6.10 Spreadsheets are not being automatically uploaded to the system, meaning manual intervention is required. System improvements are now part of the One Oracle Programme.

2.6.11 End of month Head of Service reports are not being produced, this functionality is being built into new solution as part of One Oracle.

2.6.12 The Accounts Receivable system is not being reconciled on a daily basis; however developments in this area are now part of One Oracle.

2.6.13 **Audit Opinion**

2.6.14 As a result of this audit we have raised two medium and one low priority recommendations relating to:
- Procedures for the administration of Accounts Receivable to be completed; *(Low Priority)*

- Members of Accounts Receivable staff to sign Declarations of Interest; *(Medium Priority)* and
- Data Protection & money laundering training to be made available and procedures documented. *(Medium Priority)*

2.6.15 **Substantial Assurance** has been given as while there is a basically sound system, there are limitations that may put some of the systems objectives at risk, and/or there is evidence that the level of non-compliance with some of the controls may put some of the system objectives at risk.

2.7 Background

2.7.1 Modern.gov is an application used within local government which has numerous facets designed to support council committee processes. Principal among these functions is the ability to bring together reports from various council services and effectively collate and present them in physical and electronic form to support council Committee Administration (this process, and its interaction with supporting technology, is mapped in Appendix 1). The application also acts as an interface for internal staff and members of the general public to interact with the uploaded media.

2.7.2 The focus of this audit is primarily on assessing the security in place on the Modern.gov application. In addition, the wider system in which Modern.gov operates will be assessed with a focus on both technical and operational elements.

2.7.3 Summary of Audit Findings

2.7.4 No application report could be provided to us of different modern.gov access permissions or views associated to each access Type.

2.7.5 The allocation of *Democratic Services Administrator* type privileges does not comply with the *Principle of Least Privilege* (POLP), at this level of application usage the distribution of access permissions is insufficiently granular.

2.7.6 Havering does not currently require third parties to sign a Code of Connection (CoCo) agreement, indicating compliance with the behavioural and security requirements of the council. Penetration testing at Newham identified weaknesses with the Modern.gov application system which may impact upon the application system build used at Havering council.

2.7.7 A Single Sign On (SSO) model is adopted which utilises the modern.gov interface with Microsoft Active Directory. All access to the application is granted on the operating system layer. The reliance on the operating system authentication does introduce a degree of risk, for instance unauthorised access is made possible if operating system access is granted and the workstation is left unattended.

2.7.8 The Committee Administration team have no involvement with the contractual elements governing the Modern.gov application even though as primary users they are best placed to appraise the level of service delivered by Modern Mindset.

2.7.9 The Application Control structure has not been formally mapped and a Fit for Purpose Review is not performed annually but it is a dynamic and constant process. The product is constantly evolving; the Committee Administration team works with Modern Mindset to develop the application.

2.7.10 The current build in use at Havering is Modern.gov 1250 - this is not the latest version. Currently the decision making process in relation to patch/update implementation lies with the Committee Administration team which may not have the necessary expertise to identify critical system updates.

2.7.11 The management of leavers is not informed by up to date intelligence on leavers, for example leaver reports from the Havering HR system. There is a risk that employees could use the login details of leavers to access Modern.gov resources, diminishing accountability.

2.7.12 Services were identified using old templates leading to information omissions, this being likely to be an issue relating to version control over report templates although clear guidance has been provided to services on approaches to handling exempt and confidential reports.

2.7.13 The current back-up policy for the server upon which Modern.gov sits is a daily backup which is retained for 10 days; this is a short term backup solution.

2.7.14 The service was unable to provide assurances that default passwords on the built-in generic Administrator account had been changed. This account only had Councillor type permissions which are limited.

2.7.15 Four Active Directory role groups were identified which were attributed to Modern.gov but did not have any permissions allocated to them.

2.7.16 **Audit Opinion**

2.7.17 As a result of this audit three high, seven medium and two low priority recommendations have been raised.

2.7.18 Recommendations related to the need for:

2.7.19 Committee Administration should liaise with the developer to identify with absolute clarity the specific capabilities of each user *Type*. Users should only be placed in role *Types* which reflect the specific application usage needs of their post. (*High Priority)*

2.7.20 A review should be performed of all Democratic Services Administrator access provided to users. There should be a valid business case for all administrator access issued which conforms to the Principle of Least Privilege. Access should be restricted to reflect role requirements. (*High Priority)*

2.7.21 Committee Administration should liaise with ICT and Modern Mindset to identify whether their build is affected by security weaknesses and, if required, the necessary action taken to mitigate these risks. A Code of Connection agreement with Modern Mindset should also be introduced. *(High Priority)*

2.7.22 The department should ensure it completes the transition to adopting Microsoft best practice guidelines as soon as possible. *(Medium Priority)*

2.7.23 Ownership for the contractual management over Modern.gov should be identified. The Committee Administration team should obtain a copy of the Service Level Agreement from ICT and play an active role in monitoring the service provide. *(Medium Priority)*

2.7.24 It would be beneficial to map application responsibilities out in the event of any unexpected personnel changes and clarity should be established as to which party is responsible for assessing the application fitness for purpose. *(Medium Priority)*

2.7.25 Modern Mindset should be contacted to ensure any patches/updates issued following the current implemented version do not fix a security weakness within the application. If a critical patch/update is identified it should be implemented with liaison with ICT and ensure that a proper Change Management process is followed. *(Medium Priority)*

2.7.26 Leaver management within the application system should be informed by leaver reports generated by the council's HR system. Frequent reconciliations should be performed to ensure unauthorised access is removed promptly. *(Medium Priority)*

2.7.27 The introduction of periodic user notifications (e.g. biannual) may be beneficial. As part of any periodic notifications it would be useful to reinforce end user usage of templates and ensure end users are using the correct version of templates. *(Medium Priority)*

2.7.28 The service should assess the appropriateness of the short term back-up solution in light of the criticality of the application system and appropriate action taken. *(Medium Priority)*

2.7.29 All generic passwords are changed. New passwords should be 'strong', confidential and stored securely in the event of application system failure. *(Low Priority)*

2.7.30 ICT should liaise with Modern Mindset to identify the purpose of the role groups attributed to Modern.gov that do not have any associated permissions. If there is no future requirement for the existence of these role groups they should be terminated. *(Low Priority)*

2.7.31 A **Substantial Assurance** opinion has been issued for the following reasons:
   • Overall, the inherent risk of the application system to the organisation was not perceived as significant. The application has been implemented in its simpler form, thus reducing the associated risk. However, the Committee Administration team wishes to implement a partially decentralised model in the medium term future. Responsible officers

should be mindful that the risk profile of the application will change with this new model;

- Numerous strength areas were noted, these are identified on the overleaf page;
- In one case, where a critical high risk control weakness was identified mitigating controls were in place which reduced the level of risk; and
- DPA conflicts were identified in one case.

2.8   Background

2.8.1   As part of maintaining IT applications, software releases are issued by suppliers. These releases are often planned and can contain functionality upgrades or error clearance solutions.

2.8.2   Change control procedures are designed to ensure that no unauthorised changes (including releases of software) are made to IT systems. Failure to manage change control processes has resulted in critical failures in some large organisations; for example, recent failures in the banking sector have been well publicised.

2.8.3   Information and communications technology (ICT) is vital to the effective operation of all spheres of activity within the Council. In order to deliver services, the council utilises a large number of IT applications. These are managed by ICT Services, which use the following as best practice tools:
- ITIL (Information Technology Infrastructure Library), which defines the purpose of the change management process as 'controlling the lifecycle of all changes, enabling beneficial changes to be made with minimum disruption to IT services'.
- The security standard ISO17799, which includes systems development and maintenance within its 10 primary control areas. An operating system (OS) is a collection of software that manages computer hardware resources and provides common services for computer programs. The operating system is a vital component of the system software in a computer system.

2.8.4 Summary of Audit Findings

2.8.5   Various policies are in place, however, there are no detailed audit trail requirements and ICT analysts' practices vary.

2.8.6   There are no standard checklists in use or quality control system in place.

2.8.7   In respect of a documented audit trail:
- No standard audit trail process exists;
- There is no access to third party test plans or records; and
- There is over-reliance on e-mail accounts for document storage.

2.8.8 Audit Opinion

2.8.9   As a result of this audit three high priority recommendations have been raised.

2.8.10 Recommendations related to the need for:

2.8.11 A review of policies and procedures operated at both sites should be carried out with a view to all working to a single set of guidance. Once the single set

of guidance has been agreed a short training brief should be issued to all ICT Analsysts.

2.8.12 The requirement to maintain an audit trail of activity, in relation to software releases, and the tools and locations to be used for this, should be explicit within the Joint Change Management Policy or a new joint Change Management Process.

2.8.13 A system of quality control is introduced.

2.8.14 As a result of our findings, the audit opinion is **Limited Assurance**.

2.9   Background

2.9.1   An operating system (OS) is a collection of software that manages computer hardware resources and provides common services for computer programs. The operating system is a vital component of the system software in a computer system.

2.9.2   The purpose of this operating system audit is to establish whether the configuration, security and management of the OS is effective, robust, in-line with corporate standards and policies and meets best practice. This audit focused on testing the operating systems of the two domain controllers (DC's) located at London Borough of Havering's Town Hall.

2.9.3   Three areas that were part of the original audit scope for this audit were either not tested or not tested in any detail. This was due to these areas already having been the subject of testing in the previous audit of Network Permissions. These areas are noted below. However, please refer to the audit on Network Permissions for the detailed findings and recommendations.
- Monitoring of Audit Logs:
- Audit Log Configuration Settings:
- Systems Administrators Access to the Domain Controllers:

2.9.4   **Summary of Audit Findings**

2.9.5   Corporate procedures have not been documented that cover all the key security functions, policies and standards and communicated to all personnel involved in the administration of security for the operating system

2.9.6   A process is not in place to ensure that individuals with security administration responsibilities are promptly kept informed of key system weaknesses and vulnerabilities through affiliation to relevant websites and security forums.

2.9.7   Best practice security standards have not been defined as the Council's corporate standard; neither have the operating system's configuration settings been set to high security on the domain controllers.

2.9.8   The operating system security parameters have not been correctly configured to offer adequate security protection to the system. This means that the configuration is not compliant with best practice.

2.9.9   Outputs from the Nessus reports need to be examined and the necessary action should be taken to guard against malicious hackers (or crackers) using open ports to attempt to exploit potential vulnerabilities.

2.9.10   The system configuration for the DCs did not receive prior approval from the relevant manager before, or after, their release into the production environment.

2.9.11 It was identified that warnings were not present when accessing the domain controllers and were only present on outward facing systems in the Demilitarised Zone (DMZ).

2.9.12 **Audit Opinion**

2.9.13 As a result of this audit five high and two medium priority recommendations have been raised.

2.9.14 Recommendations related to the need for:

2.9.15 Policies and procedures that detail the key security attributes of the network should be documented (i.e. system configuration settings, administrator access levels, remote access protocols and the process for audit log monitoring). Policies should be updated annually and made available to all relevant personnel involved in security administration and configuration of systems on the Council's network. (*High Priority*)

2.9.16 Officers involved in security administration for the Council should be signed up members of advisory and vulnerability websites, and the vulnerability reporting services of the Information Security for London (ISFL) WARP, which they are members, to ensure that they are promptly notified when system vulnerabilities and weaknesses are identified. (*High Priority*)

2.9.17 A review of the weak security settings, currently present on the DCs, should be performed immediately. A business case should be documented where it is deemed that changing a particular setting will have an impact on the stability of the system, which should also include what alternative method of security has been identified or whether the risk is to be accepted. (*High Priority*)

2.9.18 The automatic updates should be enabled and correctly managed by defining whether to be notified when new updates are available and choosing whether to install them or not. This process can also be managed through the Group Policy Object (GPO). The Windows firewall should be correctly enabled and configured on both domain controllers; c) The internet explorer zones for the user "stevensk" should have both the ActiveX script and Java permissions identified above disabled, unless there is a strong business case for maintaining this setting. (*High Priority*)

2.9.19 The Nessus reports should be examined on a monthly basis and the necessary action taken to rectify any weaknesses identified. Action taken to resolve issues should be appropriately recorded and where it is deemed that no action is required a detailed explanation of the reason for no action should be recorded and maintained in line with the Council's retention policy. (*High Priority*)

2.9.20 System configurations should always receive prior approval from the relevant senior manager before they are officially released into the production environment. (*Medium Priority*)

2.9.21 Warning banners should be present on all of the Council systems, notifying individuals that unauthorised access and inappropriate use of the system may result in subsequent prosecution. (*Medium Priority*)

2.9.22 Based on the work and testing performed, the operating system(s) has been given a **Limited Assurance** assessment due to the level of weakness identified within the control environment.

2.10 Background

2.10.1 In 2011/12 the Contract Procedure Rules were reviewed and amended. The threshold before which it is mandatory within Council Policy to seek support from the Internal Shared Service specialist procurement resources has been increased to £100k.

2.10.2 The threshold was increased as a result of a regional strategy for all boroughs, in London, to work towards aligning thresholds for going out to tender, in order to increase opportunities to procure in partnership. It was also considered that the cost of undertaking a full procurement process was at times greater than the financial benefit and was not sufficiently considering risk. In addition, to achieve savings, the back office support services in the Council have been reduced with the introduction of new technology and a move to a culture of manager self-service.

2.10.3 In 2012/13 the Council has implemented a new IProcurement system this will increase the control over expenditure and in particular the management information available to inform decisions and future strategy and efficiency in ensuring compliance.

2.10.4 **Summary of Audit Findings**

2.10.5 An analysis of the spend data available was undertaken as part of the audit , this showed that there were over 200 suppliers where overall spend of over £100k during 2012/13 who were not present on the contracts register. Going forward the IProcurement system will assist in identification of high expenditure with one supplier but a recent audit indicated that the service is not yet out of the implementation phase and onto Business as Usual so some controls are yet to be implemented.

2.10.6 Several services had no staff attendance at training supplied by Operational Procurement in 2011/12 when the Contract Procedure Rules were amended. This weakness in ensuring training is appropriately attended has been acknowledged by the organisation. All training is now booked, approved and attendance monitored via the Oracle Learning Management Module and although it is still line management that will enforce compliance the management information to support this is now complete and timely and with the introduction of self service workforce capability has become a focus for Senior Management. Heads of Service are responsible for ensuring that all officers are sufficiently skilled and trained to undertake corporate core activities. Failure by officers to comply with Council Policy is covered by the Council's disciplinary processes.

2.10.7 **Audit Opinion**

2.10.8 As a result of this audit one medium priority recommendation has been made relating to:
- Analysis of high spend suppliers to be carried out

2.10.9 **Substantial Assurance** has been given as while there is a basically sound system, there are limitations that may put some of the systems objectives at risk, and/or there is evidence that the level of non-compliance with some of the controls may put some of the system objectives at risk.

Section 3 Schools Audit Work

Five Schools audits were undertaken in quarter four but the final report was issued after the 31st March 2013. Results of the audits are included in Schedule 2 below.

Management summaries will only be included in the quarterly progress reports when we have given limited or no assurance.

Schedule 2: 2011/12 – School Audits Completed

Report	Opinion	Recommendations				Ref Below
		High	Med	Low	Total	
Dame Tipping CE Primary	Substantial	0	3	3	6	N/A
Rise Park Infant School	Substantial	0	3	0	3	N/A
Rise Park Junior School	Substantial	1	5	1	7	N/A
Chafford	Substantial	2	5	1	8	N/A
Sanders Draper	Substantial	2	5	3	10	N/A

Section 4 – Outstanding Recommendations Summary Table

Categorisation of recommendations

High: Fundamental control requirement needing implementation as soon as possible
Medium: Important Control that should be implemented
Low: Pertaining to Best Practice

4.1   Outstanding Internal Audit Recommendations

Review in	Area Reviewed	HoS Responsible	Outstanding			Position as at end May 13		
			High	Medium	Low	In Progress	Not Started	Position Unknown
2008/09	Cemeteries & Crematorium	Housing & Public Protection		1		1		
		2008/09 Total		1		1	0	0
2009/10	Climate Change	Culture & Community		1		1		
		2009/10 Total		1		1	0	0
2011/12	Public Protection	Housing & Public Protection			1	1		
2011/12	Remote Working	Business Systems		1		1		
2011/12	Oracle Financials	Business Systems		3		3		
2011/12	Crematorium – Grave Allocations & Record Keeping	Housing & Public Protection		4		4		
2011/12	Education Computer Centre	Business Systems	3	3		6		
2011/12	Appointeeship & Deputyship	Adult Social Care	1			1		
2011/12	Network Infrastructure	Business Systems	1			1		
2011/12	Pensions	Shared Services		1		1		
2011/12	i-Expenses & Purchase Cards	Group Director – F&C	1			1		
2011/12	i-Expenses & Purchase Cards	Shared Services	1	1	1	3		

Review in	Area Reviewed	HoS Responsible	Outstanding			Position as at end May 13		
			High	Medium	Low	In Progress	Not Started	Position Unknown
2011/12	Main Accounting	Shared Services		1		1		
2011/12	Oracle Financials	Business Systems / Shared Services		3		3		
		2011/12 Total	**7**	**17**	**2**	**26**	**0**	**0**
2012/13	Oracle Financials	Business Systems / Shared Services		2	2	4		
2012/13	Information Governance	ACE – Legal & Democratic Services	1	1		2		
2012/13	Network Permissions	Business System	1			1		
2012/13	Parking: Cancellation of PCN's	Streetcare			1	1		
2012/13	i-Recruitment	Strategic HR & OD	1			1		
2012/13	Transport	Asset Management		1		1		
2012/13	Modern Governance	ACE – Legal & Democratic Services	1	3		4		
		2012/13 Total	**4**	**7**	**3**	**14**	**0**	**0**