Appendix 1

Progress Report - Internal Audit Reports Issued since 1st April 2012

Audit's that have been finalised since the last progress report to the Standards & Audit Committee and their Audit Assessments are as follows:

Audit Reviews

Description of Audit	Assurance Level
Beacon Hill School	Green
Council Tax	Green
Dikkes Primary School	Green
Holy Cross Catholic Primary School	Green
Stifford Clays Infant School	Green
Stifford Clays Junior School	Green
St Joseph's Catholic Primary School	Green
Thameside Infant School	Green
Thameside Junior School	Green
Kenningtons Primary School	Amber/Green
West Thurrock Primary School	Amber/Green
The Grays School Media Arts College	Amber/Red
Care Proceedings	Amber/Red
IT Vulnerability Management	Red

Management summaries and action plans for reports issued with an Amber/Red or Red assurance opinion are shown below.

The Grays School Media Arts College

1 EXECUTIVE SUMMARY

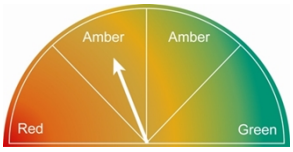
1.1 INTRODUCTION

An audit of Grays School Media Arts was undertaken as part of the approved internal audit periodic plan for 2011/12.

The audit was designed to assess the controls in place to manage the following objectives and risks:

Objective	To ensure the school is administered in the most economic, efficient and effective way possible in accordance with Central Government and Local Authority guidelines.
Risk	Controls over the school's bank account(s) and governance are weak resulting in financial loss to the school. Controls over the school's petty cash funds are weak resulting in financial loss to the school. Procurement is not controlled resulting in inappropriate purchases of goods and services. Staff are not informed of how to purchase, store or dispose of fixed assets. There is an inadequate separation of duties for making changes to personnel data. Repairs and maintenance are not kept up to date and do not achieve value for money. Income due to the school is not appropriately recorded and as such is not collected in full. The school's budget is not balanced or aimed at recovering a deficit or achieving a prudent level of unspent balances resulting in inefficient use of school funds. The school does not have valid insurance policies in place which may lead to financial loss in the event of claims being made. Security of school data is not adequately controlled leading to a loss of information or breach of confidentiality.

1.2 CONCLUSION



Taking account of the issues identified, whilst the Governing Body of Grays School Media Arts can take some assurance that the controls upon which the organisation relies to manage this risk are suitably designed, consistently applied and effective, action needs to be taken to ensure this risk is managed

The above conclusions feeding into the overall assurance level are based on the evidence obtained during the review. The key findings from this review are as follows:

- The Copy of the Financial Regulations held in the office is neither signed nor dated.
- The re-appointment of the private fund auditor has not been approved by the Governors.
- Petty Cash claims are not submitted each month.
- Purchase Orders are not always raised before receipt of the invoice.
- The schools inventory is not dated or signed, and no costs included.
- It is not clear if computer equipment is security tagged.
- Copies of contracts held must be dated and signed
- Invoices for lettings must be despatched each month.
- The School Improvement Plan does not incorporate a 3-year plan.

- The inclusion in the Information Commissioners register is not up to date.

1.3 SCOPE OF THE REVIEW

To evaluate the adequacy of risk management and control within the system and the extent to which controls have been applied, with a view to providing an opinion. Control activities are put in place to ensure that risks to the achievement of the organisation's objectives are managed effectively. When planning the audit, the following controls for review and limitations were agreed:

Limitations to the scope of the audit:

- Testing will be undertaken on a sample basis only. Our work does not provide any guarantee against material errors, loss or fraud or provide an absolute assurance that material error, loss or fraud does not exist.

The approach taken for this audit was a Risk-Based Audit.

1.4 RECOMMENDATIONS SUMMARY

The following tables highlight the number and categories of recommendations made. The Action Plan at Section 2 details the specific recommendations made as well as agreed management actions to implement them.

Recommendations made during this audit:

Our recommendations address the design and application of the control framework as follows:

	Priority		
	High	Medium	Low
Design of control framework	0	0	0
Application of control framework	0	3	7
Total	**0**	**3**	**7**

The recommendations address the risks within the scope of the audit as set out below:

	Priority		
Risk	**High**	**Medium**	**Low**
Controls over the school's bank account(s) and governance are weak resulting in financial loss to the school.	0	0	2
Controls over the school's petty cash funds are weak resulting in financial loss to the school.	0	0	1
Procurement is not controlled resulting in inappropriate purchases of goods and services.	0	1	0
Staff are not informed of how to purchase, store or dispose of fixed assets.	0	0	2
There is an inadequate separation of duties for making changes to personnel data.	0	0	0
Repairs and maintenance are not kept up to date and do not achieve value for money.	0	1	0
Income due to the school is not appropriately recorded and as such is not	0	1	0

	Priority		
Risk	**High**	**Medium**	**Low**
collected in full.			
The school's budget is not balanced or aimed at recovering a deficit or achieving a prudent level of unspent balances resulting in inefficient use of school funds.	0	0	1
The school does not have valid insurance policies in place which may lead to financial loss in the event of claims being made.	0	0	0
Security of school data is not adequately controlled leading to a loss of information or breach of confidentiality.	0	0	1
Total	**0**	**3**	**7**

Recommendations implemented since the previous audit in this area:

Date of previous audit: 2 November 2009			
Assurance:	**Fundamental**	**Significant**	**Merits Attention**
Number of recommendations made during previous audit	0	3	13
Number of recommendations implemented	0	2	8
Recommendations not yet fully implemented:	**0**	**1**	**5**

2 ACTION PLAN

The priority of the recommendations made is as follows:

Priority	Description
High	Recommendations are prioritised to reflect our assessment of risk associated with the control weaknesses.
Medium	
Low	
Suggestion	These are not formal recommendations that impact our overall opinion, but used to highlight a suggestion or idea that management may want to consider.

Ref	Recommendation	Categorisation	Accepted (Y/N)	Management Comment	Implementation Date	Manager Responsible
1.4	The Financial Regulations need to be signed by the Chair of Governors at the time of the meeting when it is approved. A signed and dated copy must be held at the school	Low	Y	This will be added to the next meeting's agenda	Spring 2012	Chair
1.5	The approval of the auditor for the School Fund needs to be included in the agenda for the next Governors meeting.	Low	Y	As above	Spring 2012	GB
2.2	Petty Cash claims should be submitted to Thurrock Council either once a month or when the amount reaches £200, whichever is the sooner.	Low	Y	The Office will start sending in the claims either each month or when the amount reaches £200	Spring 2012	Bursar/Finance Officer
3.1	Purchase Orders must be raised on the system and authorised by the appropriate personnel, before a requisition for goods is placed with the supplier. This is in accordance with the Financial Regulations and ensures management information reports are up to date.	Medium	Y	This will be passed to the Governors. The Finance Office have made several requests to be made aware of goods/services required in the first instance	A.S.A.P	Head/Chair

Ref	Recommendation	Categorisation	Accepted (Y/N)	Management Comment	Implementation Date	Manager Responsible
4.1	The cost price or estimated current value of equipment should be included on the inventory; All pages should be signed and dated to show when the inventory was last checked.	Low	Y	This will be passed to the Network Manager	A.S.A.P	Network Manager/Bursar
4.3	Equipment needs to be re-checked to ensure that it has been security marked and an identification sticker placed on the equipment.	Low	Y	As above	A.S.A.P	Network Manager
6.1	Copies of all contracts must be retained and they must be signed and dated. This shows value for money is being obtained and provides evidence if a dispute arises.	Medium	Y	We will ensure copies of all new contracts held in the office are signed and dated.	When new contract drawn up	Bursar
7.2	Invoices should be raised on a monthly basis for all lettings at the school. This reduces the likelihood of loss of revenue to the school through non-payment.	Medium	Y	In future invoices will be sent out each month.	A.S.A.P	Bursar
8.4	The School Development Plan should cover the next 3 years, with 2012-2013 being a detailed plan and the additional 2 years an indicative plan of expected development activities and budgets. This assists the school in planning in the longer term.	Low	Y	The Bursar commented on behalf of the Head Teacher. The Head Teacher is currently writing a new plan	Summer Term	Head Teacher
10.1	The renewal for the re-entry into the data protection register, needs to be sent off as soon as possible	Low	Y	The application to renew the entry into the register has now been posted	April 2012	Bursar

Care Proceedings

1 EXECUTIVE SUMMARY

1.1 INTRODUCTION

An audit of Care Proceedings was undertaken as part of the approved internal audit periodic plan for 2011/12.

If the Council has serious concerns about the safety or welfare of a child, it can apply to the court to take the child into care. Children are only taken into care when Social Services are really worried that they are suffering, or are likely to suffer, significant harm from the way they are being looked after by their parents or carers, or where the child is beyond the control of a parent.

The Expenditure on Care Proceedings for the last 4 years was £1,947,131 as per following breakdown:-

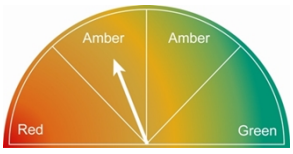
2008-09	£423,651	(no. of cases not provided)
2009-10	£449,642	(48 cases)
2010-11	£613,014	(28 cases)
2011-12	£460,824	(42 cases)

Objective	Social Workers and Legal Services are working closely and effectively together
Risk	Social Workers and Legal Staff are not working effectively together and the best possible outcome for the child is not obtained.

Objective	Delays in care proceedings are minimised
Risk	Applications are submitted to the courts with missing or incomplete key documents.

Objective	Performance is monitored
Risk	Performance is not monitored

1.2 CONCLUSION



Taking account of the issues identified, whilst the Council can take some assurance that the controls upon which the organisation relies to manage this risk are suitably designed, consistently applied and effective, action needs to be taken to ensure this risk is managed.

The above conclusions feeding into the overall assurance level are based on the evidence obtained during the review. The key findings from this review are as follows:

- Social Workers and Legal Staff are working well together and proceedings are carried out with due diligence;
- Parents are notified of proceedings and efforts are made to keep the family together;
- Managers are not always made aware of Service Level Agreements between Legal and Social Care;
- Core Assessments are not always completed within the required timescales;

- A Local Performance Improvement Group has been formed and it is attended by Representatives from Legal and Social Care.
- Costs for each individual case are not monitored.

1.3 SCOPE OF THE REVIEW

To evaluate the adequacy of risk management and control within the system and the extent to which controls have been applied, with a view to providing an opinion.. Control activities are put in place to ensure that risks to the achievement of the organisation's objectives are managed effectively. When planning the audit, the following controls for review and limitations were agreed:

Limitations to the scope of the audit:

- The scope of the audit will be limited to reviewing processes in place. Conclusions will be based upon sample testing of transactions relevant to the current financial year to date. Our work does not provide any guarantee against material errors, loss or fraud or provide an absolute assurance that material error, loss or fraud does not exist.

The approach taken for this audit was a Risk-Based Audit.

1.4 RECOMMENDATIONS SUMMARY

The following tables highlight the number and categories of recommendations made. The Action Plan at Section 2 details the specific recommendations made as well as agreed management actions to implement them.

Recommendations made during this audit:

Our recommendations address the design and application of the control framework as follows:

	Priority		
	High	Medium	Low
Design of control framework	1	1	0
Application of control framework	0	1	2
Total	**1**	**2**	**2**

The recommendations address the risks within the scope of the audit as set out below:

	Priority		
Risk	**High**	**Medium**	**Low**
Applications are submitted to the courts with missing or incomplete key documents.	1	1	0
Performance is not monitored	0	1	1
Social Workers and Legal Staff are not working effectively together and the best possible outcome for the child is not obtained.	0	0	1
Total	**1**	**2**	**2**

2 ACTION PLAN

The priority of the recommendations made is as follows:

Priority	Description
High	Recommendations are prioritised to reflect our assessment of risk associated with the control weaknesses.
Medium	
Low	
Suggestion	These are not formal recommendations that impact our overall opinion, but used to highlight a suggestion or idea that management may want to consider.

Ref	Recommendation	Categorisation	Accepted (Y/N)	Management Comment	Implementation Date	Manager Responsible
1.2	When conflicting advice is given by solicitors in the same case, the client department should notify the Head of Legal Services so she can look at the issue and ensure accurate, consistent advice is provided.	Low	Y	Efforts are being made to ensure that the solicitor with conduct of the case attends all meetings relating to the case to avoid conflicting advice being given.	Implemented.	Service Manager for Looked After Children and Service Manager for Safeguarding
2.3	Once the new People Services SLA is agreed, it should be cascaded down to Managers. This will ensure that they are aware of what is included in the services provided by Legal.	Medium	Y	A new People Services SLA will be issued shortly	Once the new People Services SLA is agreed. September 2012	Business Support Manager for Legal Services and Principal Solicitor.
2.4	More care should be taken to ensure that core assessments are completed within the timescales as their absence may delay court proceedings and will impact upon the reputation of the Council.	High	Y	People Services (Children Services) and Legal Services are working together to ensure that unless care proceedings have to be issued urgently that the core assessment has been completed.	Implemented	Service Manager for Safeguarding Service Manager for Looked After Children and Principal Solicitor

Ref	Recommendation	Categorisation	Accepted (Y/N)	Management Comment	Implementation Date	Manager Responsible
3.2	The Service Manager should meet with the Principal Solicitor to review and agree actions within the Local Performance Improvement Group Action Plan.	Low	Y	The meeting has taken place and the Service Manager is in the process of drafting the Action Plan	Implemented	Service Manager and Principal Solicitor
3.4	Full case reference and/or name should be quoted for each payment made. This information would not only provide a clear audit trail but would be useful management information, especially in view of the fact that the cases are becoming more and more expensive. All associated Care Proceeding costs should be allocated to the same code to allow the total cost of proceedings to be identified.	Medium	Y	The full case name is inserted when raising a purchase order, however, when this is submitted for approval to the Service Manager, Oracle does not appear to provide the case name.	Implemented	Service Manager and Principal Solicitor

IT Vulnerability Management

1 EXECUTIVE SUMMARY

1.1 INTRODUCTION

An audit of IT Vulnerability Management was undertaken as part of the approved internal audit periodic plan for 2011/12.

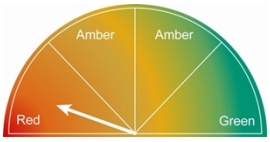
Thurrock Council ('the Council') has entered into a contract with Vertex that includes management of its ICT services. The contract began in 2005 and operates to 2020. The contract is managed for the Council by the Head of Business Services.

The Council is connected to the UK Government Connect Secure Extranet (GCSx) and the Code of Connection identifies a requirement for periodic independent vulnerability testing. The September 2011 testing identified a large number of vulnerabilities on the Thurrock Council network including a large number of servers that use operating systems that are no longer supported by Microsoft. Remediation action plans have been produced and several issues have been addressed, but not the obsolete operating systems.

The audit was designed to assess the controls in place to manage the following objectives and risks:

Objective	IT controls have been designed to ensure that the Council has implemented a secure environment for the systems that support key services to residents.
Risk	The Council's network is vulnerable to cyber threats that may lead to a loss of data or affect services

1.2 CONCLUSION



Taking account of the issues identified, the Council cannot take assurance that the controls upon which the organisation relies to manage this risk are suitably designed, consistently applied or effective. Action needs to be taken to ensure this risk is managed.

The above conclusions feeding into the overall assurance level are based on the evidence obtained during the review. The key findings from this review are as follows:

Design of control framework

The following key controls have been designed:

- Specialised software, Privilege Guard, restricts Council employees from installing unauthorised application software on their workstations, thereby reducing the risk that malware or unlicensed software is introduced to the Council's network.
- Change management policies are designed to control changes to the Council's infrastructure are in place, reducing the risk of a loss to ICT infrastructure security and availability.

However, we did identify a number of weaknesses in the design of network controls that impact network security, principally:

- The framework for ICT contract is weak as there is no governance body for the ICT service and no corresponding Service Level Agreement (SLA), increasing the risk that Council management will not be aware of operational performance or security issues.
- There are a number of servers running unsupported operating systems and there is no strategy to fund upgrades to obsolete server infrastructure or application software to remediate security vulnerabilities. This leads to a risk that Council security may be breached and there may be significant data loss.

Operating system	Number of servers	Microsoft ceased support
Windows NT 4.0	2	2004
Windows 2000	28	2010

- Although Anti-virus signature updates are distributed to servers and workstations, there are weaknesses in the process to manage exceptions, leading to devices on the Council's network excising that lack the latest anti-virus protection. In addition, there is inadequate provision of anti-virus software on servers running the obsolete versions of Microsoft Windows and the servers are vulnerable to malware infection.
- The arrangements for commissioning of network vulnerability scans and the remediation of issues raised by the scanning process have not been formalised. This increases the risk that the Council may experience unavailability of systems due to external attack following identified issues that have not been addressed.
- There is a patching policy for devices running Microsoft software but not for other software, increasing the risk that the Councils desktops may become unavailable due to exploitation of known vulnerabilities on desktop application products.
- There is an absence of an adequate ICT Risk identification, assessment or management process, increasing the risk that the Council's management will not be aware of ICT risks and those risks not being accepted or mitigated.

Application of and compliance with control framework

Overall, our testing found that a number of controls identified and evaluated during this audit are operating and being complied with, in particular:

- We confirmed that Microsoft workstations patches are automatically pushed out to the corporate test group and are then implemented across the rest of the infrastructure.
- We confirmed that the change management process had been complied with for the server patches that were deployed during three weeks of December 2011.

However, we did identify one area for management attention, principally that security patching of the Council's server infrastructure has not been performed in a timely manner (it appears to have been in reaction to the vulnerability scan results) and increases the risk that the Councils servers may become compromised through known vulnerabilities.

1.3 SCOPE OF THE REVIEW

To evaluate the adequacy of risk management and control within the system and the extent to which controls have been applied, with a view to providing an opinion. Control activities are put in place to ensure that risks to the achievement of the organisation's objectives are managed effectively. When planning the audit, the following controls for review and limitations were agreed:

Control activities relied upon:

- Server and Workstation patching.
- Change Management for the Information Technology infrastructure.
- Anti-virus on Server, Workstation, Email and Web infrastructure.
- Software installation by unauthorised users.
- Network vulnerability security assessments.

Limitations to the scope of the audit:

- The review was limited to the Areas of Consideration, identified above. Therefore, the review will not provide assurance that all aspects of IT security are being complied with or are operating effectively.
- We did not perform substantive testing where weaknesses in the design and operation of controls are identified.
- Recommendations may be informed by sample testing therefore our work does not provide any guarantee against material errors, loss or fraud or provide an absolute assurance that material error, loss or fraud does not exist.

The approach taken for this audit was a Risk-Based Audit.

1.4 RECOMMENDATIONS SUMMARY

The following tables highlight the number and categories of recommendations made. The Action Plan at Section 2 details the specific recommendations made as well as agreed management actions to implement them.

Recommendations made during this audit:

Our recommendations address the design and application of the control framework as follows:

	Priority		
	High	Medium	Low
Design of control framework	3	3	0
Application of control framework	0	0	1
Total	**3**	**3**	**1**

The recommendations address the risks within the scope of the audit as set out below:

	Priority		
Risk	**High**	**Medium**	**Low**
The council's network is vulnerable to cyber threats that may lead to a loss of data or affect services	3	3	1
Total	**3**	**3**	**1**

2 ACTION PLAN

The priority of the recommendations made is as follows:

Priority	Description
High	Recommendations are prioritised to reflect our assessment of risk associated with the control weaknesses.
Medium	
Low	
Suggestion	These are not formal recommendations that impact our overall opinion, but used to highlight a suggestion or idea that management may want to consider.

Ref	Recommendation	Categorisation	Accepted (Y/N)	Management Comment	Implementation Date	Manager Responsible
3.1	The Partnership Operations Board should define a governance framework to facilitate management of the IT services to the Council under the contract.	High	Y	Review SLA with Serco, to ensure IT Services being delivered are in scope with Council's requirements. Where gaps exist, SBDM to identify these and implement action plan to ensure alignment of Services as per Contract, with agreement by the Partnership Operations Board. Schedule 13 provides this and is kept up to date in respect of responsibilities.	Completed but continue to review on an on-going basis.	Head of Business Services
3.2	Anti-virus protection should be implemented on all servers.	Medium	Y	AV protection is no longer available for a number of legacy servers identified to the Council. Legacy servers and associated operating systems and applications need to be upgraded to a state where AV protection can be applied. These	To be agreed.	Business & Strategic Development Manager (SBDM)

Ref	Recommendation	Categorisation	Accepted (Y/N)	Management Comment	Implementation Date	Manager Responsible
				server upgrades require funding and support from the system owner. However, this is dependent on funding available following the result of decisions around the shared services work between Thurrock and the London Borough of Barking & Dagenham (LBBD).		
3.3	As part of ref 3.1: The Council should receive periodic assurance from Vertex regarding the effectiveness of the update and distribution of anti-virus measures to servers and workstations.	N/A	Y	Monthly report to be produced by Serco and provided to SBDM advising of anti-virus updates applied to servers and workstations. SBDM to take this to the Partnership Operations Board for review and feedback.	Jan 2013	SBDM
3.4	The Server team should establish a process to keep the server list within the Antivirus management console up to date.	Low	Y	Server list maintenance will be linked to the technical change control process to capture all changes. ICT have advised that physical servers will be captured on the inventory as part of the procurement process and the server list is contained within ICT's build process and additional information is also held within the server library which is extracted from a number of different sources.	Complete	SBDM
3.5	The Council's IT strategy should provide for infrastructure upgrades identified by the vulnerability assessments, particularly obsolete non-supported operating	High	Y	The current IT Strategy outlines the current need for Infrastructure upgrades. There is a requirement for the PC Refresh Policy to re-commence	On-going	SBDM

Ref	Recommendation	Categorisation	Accepted (Y/N)	Management Comment	Implementation Date	Manager Responsible
	systems.			and this is being reviewed by the SBDM, in co-ordination with the Partnership Operations Board. However, this is linked to the transformation programme and likely to change as the programme moves forward.		
3.6	A process should be documented and approved for commissioning network vulnerability scans and for the remediation of issues identified by the scans.	Medium	Y	Serco will formally document the process for commissioning vulnerability scans, currently linked to the Code of Connection assessment cycle, and any subsequent remediation. Note some remediation may require additional TC funding.	Jan 2013	SBDM
3.7	Routine assurance should be provided to IT Management that patching of workstations and servers is effective.	High	Y	Patching success/failure information is currently captured. A specific periodic exception report will be developed and reviewed to ensure the patch cycle is adhered to	Jan 2013 to set up the process.	SBDM
3.8	An ICT Risk Management process is agreed and implemented to ensure that relevant ICT risks identified, assessed, and mitigated; with links to the Corporate Risk Register.	Medium	Y	Amalgamation of the Corporate Risk Register and ICT Risk Management process is being reviewed by the SBDM. It is dependent on the discussions being held between TC and LBBD on corporate risk and risk management as a whole. Once decisions have been made, the review can continue.	On-going	Head of Business Services