



Draft Internal Audit Annual Report 2011/12
Dacorum Borough Council



Contents

Introduction	1
Overall Summary	2
Key Themes	7
Appendix 1 - Projects with Limited and Nil Assurance 2011/12	9
Appendix 2 – Assurance Levels and Priorities	15
Appendix 3- Key to Assurance Levels	19
Appendix 4 - Statement of Responsibility	21

This report and the work connected therewith are subject to the Terms and Conditions of the contract dated 16/10/08 between Dacorum Borough Council and Deloitte & Touche Public Sector Internal Audit Limited. The report is confidential and produced solely for the use of Dacorum Borough Council. Therefore you should not, without our prior written consent, refer to or use our name or this document for any other purpose, disclose them or refer to them in any prospectus or other document, or make them available or communicate them to any other party. No other party is entitled to rely on our document for any purpose whatsoever and thus we accept no liability to any other party who is shown or gains access to this document.

Introduction

Purpose of this Report

This report summarises the work that Internal Audit has undertaken during the financial year 2011/12 and the key control environment themes identified across the Authority.

Overview of Internal Audit Approach

As Internal Audit, our role is to provide an annual assurance statement on the adequacy and effectiveness of the Authority's systems of governance, risk management and internal control.

Overview of Work Done

The Audit Plan for 2011/12 focused on high risk areas to the Council. We have liaised with senior management throughout the year to ensure that internal audit work undertaken continues to focus on the high risk areas and, in the light of new and ongoing developments in the Authority, ensures the most appropriate use of our resources.

As a result of this liaison, some changes were agreed to the plan during the year. Some projects have been added to or deleted from the Plan, others have been split into separate elements, and the timing of a number of others has been changed. Consequently, the total number of projects actually undertaken in 2011/12 was 27 (compared to 34 in the prior year) - refer Overall Summary.

We generally undertake individual projects with the overall objective of providing the Members, the Chief Executive and other officers with reasonable, but not absolute, assurance as to the adequacy and effectiveness of the key controls over a number of management's objectives. Other projects are geared more towards the provision of specific advice and support to management to enhance the economy, efficiency and effectiveness of the services and functions for which they are responsible. We also undertake IT audits, follow up audits and anti-fraud work.

All internal audit reports include our recommendations and agreed actions that, if implemented by management, will enhance the control environment and the operation of the key management controls. This report sets out the results of the work performed as follows:

- **Overall summary** of work performed by Internal Audit, including an analysis of report gradings; and
- **Key themes identified** during our work in 2011/12.

In this report we have drawn on the findings and assessments included in all internal audit reports issued in 2011/12, including those that, at this time, remain in draft. It should be noted therefore that the comments made in respect of any draft reports are still subject to management response.

Overall Summary

During the 2011/12 year, 23 (85%) of the internal audit projects were rated 'full/substantial assurance' compared with 30 (88%) in the prior year. The number of internal audit projects rated 'limited assurance' has remained the same, although the percentage has increased slightly from 12% to 15%.

Report Ratings

As in previous years, we have noted areas of improvement throughout the Authority, including better control over key financial systems resulting in fewer recommendations being raised.

We are pleased to report that we have not issued any 'nil assurance' opinions in 2011/12, and have only issued four 'limited assurance' opinions.

Significant Control Weaknesses

Internal Audit is required to form an opinion on the robustness of the internal control environment, which includes consideration of any significant risk or governance issues and control failures which have arisen during the financial year 2011/12. As such, below is a list of all priority 1 recommendations raised during 2011/12 by Deloitte Public Sector Internal Audit. Included in italics is management's response to these recommendations, together with the proposed implementation date.

Partnerships – Sports Trust Delivery Plan & Funding Approval

Recommendation: The Dacorum Sport Trust "Sportspace" should prepare a three year development plan and obtain Portfolio Holder approval for the Dacorum funding contribution.

Management response / deadline: Agreed / April 2012. The Council has drafted a Sports Policy Statement for approval by Cabinet in April. The Sportspace delivery plan and funding agreement is being developed by AD Finance. This is due to be discussed at Sportspace / DBC Annual meeting in April 2012. Once this is agreed it will be for the AD Finance to seek approval from the Portfolio Holder.

Information Security – Remote Access Controls

Recommendation: A review of remote access security controls should be performed with a view to implementing additional security controls for access connections into the Council's network.

Management response / deadline: Agreed / 31 May 2012. A policy and process review using best practice on all ICT security practices and policies will be completed by the end of March 2012. Roll out of the new procedures will also take place to ensure that procedures meet the policy. This will take place by the end of May 2012.

Information Security – Laptop Management

Recommendation: An exercise should be undertaken to identify all Council owned laptops and once identified, an inventory record should be created recording all laptop details. The database should include configuration details such as the make and model of the laptop, version of the software, who it is assigned to and the details of the asset numbering.

Once this exercise has been undertaken, the laptops should be reviewed to ensure that they meet the Council's current security requirements and have hard drive encryption, an up to date and patched operating system and up to date anti-virus software. If the reviewed laptops do not meet the expected standard, they should either be upgraded to the required specification or removed from use.

Additionally, we recommend that all new laptops issued are accompanied by relevant guidance to users such as, the Council's policy on the use and security of laptops.

We further recommend that an annual audit of the Council's hardware assets is undertaken.

Management response / deadline: Agreed / 30 April 2012. An annual review of Council equipment is conducted, the last being completed in April 2011. The next review will be over March/April 2012. The inventory will be extended this year to include Software and security running on all laptops and other ICT equipment.

Information Security – Security of Mobile Phones

Recommendation: The Council should consider a stronger and robust policy on the issue and use of mobile phones with the need for adequate security to prevent unauthorised access to information (email and data) in the event that the phone is mislaid or stolen.

Management response / deadline: Agreed / 31 March 2012. All phones are password protected and ICT completed this work in the autumn of 2011. A further review of phone security will be conducted at the same time as the policy review (March 2012). Best practice will be used to ensure the policy is up to date. Any new processes will then be implemented.

Information Security – Records and Information Management

Recommendation: We recommend that, as a minimum:

- The current Records and Information Management Policy is reviewed to ensure that it meets with the Council current requirements and usage of data;

- A periodic review is conducted to ensure that users and departments are complying with the policy, for example, on records and data management, retention and destruction;
- An exercise should be conducted to review and remove records that are no longer necessary (in compliance with the DPA) but keeping in mind any regulatory and legal requirements for retention; and
- A documented records disposal procedure should be developed which is available and distributed throughout the Council.

Management response / deadline: Agreed / 31 March 2012. We will review the current policy and update this using best practice.

Information Security – Data Sharing Protocols

Recommendation: The Council should review its current approach to information sharing with other government agencies, third parties and private providers. This should ensure that:

- A review is carried out of the data sharing protocols document that is currently in place to ensure it is updated and reflects the requirements of sharing with third party organisations;
- All Departments should be required to formally identify who they share personal data with, the frequency and the form of information that is shared; and
- All users and departments should be advised of the revised protocols and to ensure that they are followed.

Management response / deadline: Agreed / 31 May 2012. We will review the Data Sharing protocol documentation and make amendments to the protocol where required.

Project Management – this report is currently issued in draft and our comments are subject to management response.

Project Management – Terms of Reference

Recommendation: Management should draft Terms of Reference for the Improving Dacorum Programme Board/Team and ensure that roles and responsibilities, including delegated decision making processes, have been documented and approved in line with the Council Financial Standing Orders.

Project Management – Project Initiation Document (PID)

Recommendation: Management should ensure that a Project Initiation Document (PID) is fully completed and in line with the Council's Project Management (PM) guidelines.

Project Management – Project Manager

Recommendation: Heads of Service, the IDP office and Project Sponsors should ensure that there is a Project Manager allocated to each project. Where there have been changes in the governance structure, details of the new project manager should be documented and approved in line with the PM guidelines.

Project Management – Equalities Impact Assessments

Recommendation: An Equalities Impact Assessment Form (EIA) should be completed by all Project Sponsors or Accountable Officers. Once completed at initiation stage, EIA forms should be sent to Human Resources as per Project Management Guidance.

Project Management – Project Approval

Recommendation: All projects should be approved in line with delegated responsibilities and supporting documentation should be reported and retained centrally at the IDP office. In addition, copies of PIDs should be formally signed by the Head of Service; Specialists (HR, Finance; and Legal) and approval documented as part of the Corporate Management Team.

Project Management – Project Estimated Costs

Recommendation: All project costs and benefits analysis should be reviewed and approved by a Finance Officer. Supporting documentation should be retained as part of the project file.

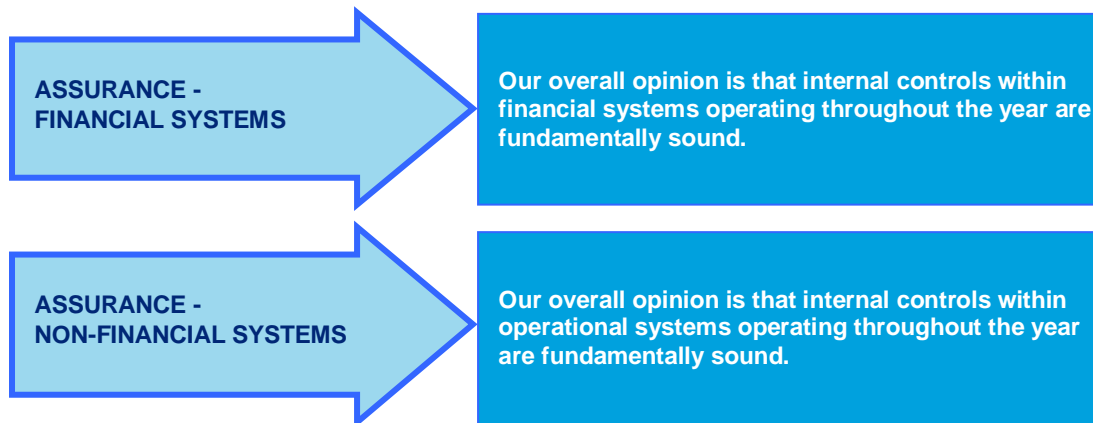
Project Management – Post Implementation Reviews

Recommendation: A Post Implementation Review (PIR) should be carried out for all projects. The accountable officer should complete and sign a PIR to agree that the report is a fair reflection of the project outcome. The report should include details on whether benefits have been achieved in line with the PID requirements.

Assurance Gradings	Number of Projects			
	2011/12		2010/11	
Full	1	4%	1	3%
Substantial	22	81%	29	85%
Limited	4	15%	4	12%
Nil	0	0%	0	0%
Sub-Total	27		34	
Merged Audits / No Opinion Audits	1		2	
Total Audits Delivered	28		36	
Audits Cancelled / Deferred	1		2	
Total	29		38	

Opinion 2011/12

From the Internal Audit work undertaken in 2011/12, it is our opinion that we can provide **Satisfactory Assurance** that the system of internal control in place at Dacorum Borough Council for the year ended 31 March 2012 accords with proper practice, except for the significant control environment issues as documented in Appendix 1. The assurance can be further broken down between financial and non-financial systems, as follows:



Key Themes

As Internal Audit continues to apply a risk based approach, our reviews assess the governance framework, the risk management process as well as the effectiveness of controls across a number of areas. Our findings on these themes are set out below. Overall, we have seen some improvements in the control environment and whilst further remedial action needs to take place, we have noted that management has already started addressing our most significant findings.

Corporate Governance

As part of our work this year, we have again completed a review of the governance arrangements in order to assist the Authority and the S151 officer in preparing the Annual Governance Statement for 2011/12. As in previous years, we have concluded that there is reasonable assurance that the Authority's governance arrangements are largely compliant with the best practice guidance on corporate governance issued by CIPFA/SOLACE.

Risk Management

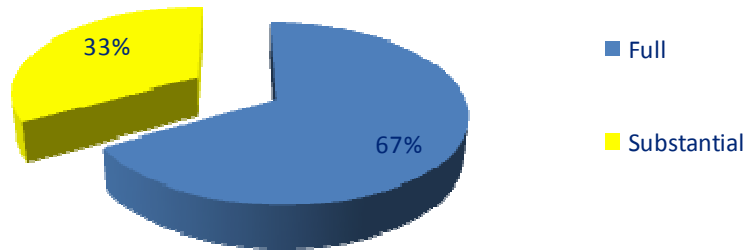
Based on an internal audit of the Authority's risk management framework, we have concluded that there is reasonable assurance that the Authority's risk management processes are sufficiently formalised and provide information on key risks and issues relating to directorates and the Authority as a whole. There has been significant change in the personnel responsible for updating registers and the registers themselves have been changed to reflect the updated structure of the organisation. However, we found there are processes for identification, recording, and reporting risks, controls, and to help identify action plans to mitigate risks to an acceptable level. The audit provided an overall substantial assurance rating, and we have raised recommendations to further enhance and embed risk management processes.

Internal Control - Key Financial Systems

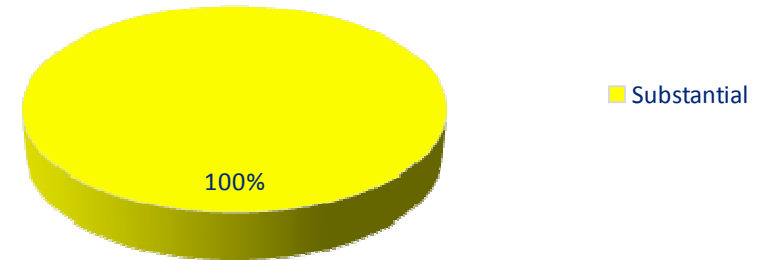
Each year Internal Audit carries out audits of the Authority's key financial systems, working in accordance with the managed audit process agreed with the Audit Commission.

This process allows the Audit Commission to place reliance on the work performed by Internal Audit to provide the Authority with the necessary assurance that key financial controls in the fundamental systems are operating satisfactorily and support a robust control environment. It also allows the Authority to limit Audit Commission fees spent on reviewing the Authority's activities. The table below summarises the audit gradings in this key area:

**Evaluation Assessment - Key Financial Systems
2011/12**



Testing Assessment - Key Financial Systems 2011/12



Overall we have seen a significant improvement in the control environment around key financial systems with regards the number of recommendations raised in each report.



As referred to in the overall summary above, and included in Appendix 1 – Projects with Limited and Nil Assurance 2011/12, we provided limited assurance for either design of controls, or application of controls, or both for four audit areas in respect of:

- Partnerships;
- Project Management (Transformation);
- Business Continuity & Disaster Recovery; and
- Information Security.

It should also be noted that whilst we highlight in Appendix 2 – Assurance Levels and Priorities the breakdown, by priority, of the recommendations raised in audit reports issued during the year, we have only raised priority 1 recommendations where we consider the issue to be fundamental to the system and upon which the organisation should take immediate action to remedy in three reports.



We have identified a number of priority 2 and priority 3 recommendations where we believe the control environment can be improved; these are detailed in the individual audit reports presented to the Audit Committee on a quarterly basis.

Appendix 1 - Projects with Limited and Nil Assurance 2011/12

Project	Evaluation Assessment	Testing Assessment	Summary of Key Findings
Partnerships	Substantial 	Limited 	<p>We have raised one priority 1, six priority 2 and one priority 3 recommendations where we believe there is scope for improvement within the control environment. These are set out below:</p> <ul style="list-style-type: none"> • There were 40 partnerships listed on the partnership register, and a Partnership Assessment Form had been completed for each. Although a full risk assessment was stated for 27 partnerships, 13 were missing from the risk register. Of the 40 partnerships listed on the main partnership register, full assessment details, such as financial commitment, were detailed for 37 but no such information was provided for the three most recent additions to the register. One of the three partnerships not included on the register was the Sports Trust, which received the highest level of funding (circa £500k per year). • Audit was not provided with evidence that a delivery plan was in place for 2011 and beyond. Similarly, there was no evidence that the actual financial commitment of £525k had been approved by the Portfolio Holder or Cabinet prior to inclusion in the annual budget. However, the funding award is reviewed by officers every year (Deputy 151 Officer, Assistant Director Strategy and Transformation, Group Manager, Sportspace Chief Executive and Finance Director). (Priority 1) • The reporting and performance monitoring arrangements between the Council and the new Strategic Partners had not been defined and communicated to all relevant partners. • There was an annual review to check if the known partnerships were still ongoing, but there was no end date documented for each partnership.

			<ul style="list-style-type: none"> • The existence and performance of partnerships was not being reviewed by any Council committee. • Partnership Assessment Forms were not being annually reviewed. • Partnership Framework documents were not made available to staff via the intranet. • The Heads of Service were requested in January 2010 to confirm the existing partnership register and to advise of any new partnerships. However, responses were not received from all areas.
Project Management (Transformation) Draft Report	Limited 	Limited 	<p>We have raised seven priority 1 recommendations and eight priority 2 recommendations where we believe there is scope for improvement within the control environment. These are summarised below:</p> <p><u>Priority 1</u></p> <ul style="list-style-type: none"> • Terms of reference detailing the roles and responsibilities of the IDP Board/Team should be drafted and approved. • Sample audit testing identified that a Project Initiation Document (PID) was not always completed and retained for all projects. • Not all projects had a clearly identifiable project manager. Where changes to project management were noted, a change control form had not been completed in line with Project Guidance documentation. • An Equalities Impact Assessment was not always completed for each project. • Project Initiation Documents were not always approved by an appropriate officer. • Project estimated costs were not always completed and approved by a Finance Lead Officer. • Post-implementation reviews were not carried out following project















			<p>completion.</p> <p><u>Priority 2</u></p> <ul style="list-style-type: none"> • For three out of the five projects selected for testing, there was no evidence to show that Project Board and Working Group meetings were minuted and that decisions had been documented as part of the project decision making process. • Two out of the five projects selected were not entered onto the CorVu system. • Change control forms were not always completed when required. • IDP guidance had not been amended to reflect the change in process regarding Status reports. • Highlights reports were not always produced and reported to management in line with guidance. • Progress on specific projects was not always reported to senior management on a regular basis. • Risk registers were not always completed and reviewed. • Lessons-learnt logs were not completed during the project life cycle.
Business Continuity and Disaster Recovery	Substantial 	Limited 	<p>We have raised seven priority 2 recommendations and one priority 3 recommendation where we believe there is scope for improvement within the control environment. These are summarised below:</p> <ul style="list-style-type: none"> • Third party agreements/arrangements where the Council relies on key suppliers and services with respect to disaster recovery for all the critical IT systems have not been included within the ICT Systems Continuity Plan. • The ICT Systems Continuity Plan does not have clear escalation procedures and details of tasks that need to be carried out during the course of a disaster event. • There are no salvage and relocation procedures in place for the

















			<p>recovery of Council systems in a disaster situation.</p> <ul style="list-style-type: none"> • The current ICT Business Continuity Plan needs to be revised to meet the Dacorum template standards. The role of ICT in other Service Business Continuity Plans needs to be further co-ordinated. • Recovery Time Objectives (RTO) have not been identified for the recovery of critical services and key IT systems. RTOs assigned to critical activities allow management to recover key systems in a way that minimises the impact on the Council and that is in line with the expectations for recovery for Council services. • Whilst Dacorum has identified points of failure regarding business system knowledge, the SOCITM review in November 2010 noted a potential weakness regarding the Dacorum Internet site. • The output from Disaster Recovery testing is not formally presented to management. Management should have the opportunity to comment or make recommendations based on test outcomes. • Backup hardware is eight years old and is becoming unreliable. We note that replacement solutions are currently being investigated.
Information Security	Limited 	Limited 	<p>We have raised five priority 1 recommendations, fifteen priority 2 recommendations and four priority 3 recommendations where we believe there is scope for improvement within the control environment. These are summarised below:</p> <ul style="list-style-type: none"> • IT Security: Security of the Council's network as well as its data and information is dependent on appropriate IT security controls being defined and policies being implemented. We looked at various areas of IT security as set out in the scope of the audit and found that, although there are controls and policies in place, these should be enhanced to improve security and provide a greater level of protection. For example, we have recommended that the network password controls be improved, greater audit logging and monitoring is performed, additional

















			<p>authentication is introduced for remote access, the requirement to perform a laptop asset audit to help ensure that the latest security controls have been employed on all portable PCs, similarly all mobile phones that have an email and data capability should have additional protection such as passwords and encryption enforced when issued as standard. In addition, we have also recommended that only approved Council issued encrypted USB devices be permitted.</p> <ul style="list-style-type: none"> • Information Security and Governance: We performed audit testing on the Information Security Policies, roles and responsibilities over Information, Data Classification and Asset Ownership. As a result of our audit, we identified that currently Information Asset Owners have not been identified for Council information, that there is no process in place to identify and classify data according to its sensitivity. We also identified that there is no formal records management process in place. Our audit identified that although a data sharing protocol is in place, this was created in 2001 and has not been reviewed for some time. In addition, we could not identify who had signed up to the protocol. Although the Council has a number of policies and procedures established for Information Security, these could benefit from consolidation into a single document covering all major areas of IT related security. We also have recommended that the ownership of this document be formally assigned as the Information and data sharing protocols and agreements in place have not been reviewed for a long time to confirm validity and adequacy and since the departure of the Information Security Officer, there is currently no specific designated Security Officer in post. This role is currently performed by an IT officer who apart from this role and their other IT roles is also designated as the Records and Data Management officer. • Site Visits:
--	--	--	---









			<p>As a result of the original information security incident, we also visited three randomly selected sites within the Council – Chaulden Children’s Adventure Playground, Berkhamstead Civic Centre and the Woodwell Cemetery. Some of the issues identified include records created on spreadsheets or databases that are not protected, records are retained longer than necessary, and access to files and folders is not restricted.</p>
--	--	--	---

Appendix 2 – Assurance Levels and Priorities

Project	Evaluation Assessment	Testing Assessment	Status	Priority		
				1	2	3
Corporate Governance	Full 	Substantial 	Final	0	2	0
Risk Management	Substantial 	Substantial 	Final	0	3	3
Environmental Health/Food Safety	Substantial 	Substantial 	Final	0	4	1
Complaints Handling	Substantial 	Substantial 	Draft	0	4	0
Health and Safety – Follow Up	N/A	N/A	Complete	-	-	-
HRA Self-Financing	Full 	Full 	Final	0	0	0
Main Accounting	Full 	Substantial 	Draft	0	0	1
Budgetary Control	Full 	Substantial 	Final	0	1	1

Project	Evaluation Assessment	Testing Assessment	Status	Priority		
				1	2	3
Accounts Payable	Full 	Substantial 	Final	0	2	1
Payroll	Full 	Substantial 	Final	0	2	1
Council Tax	Substantial 	Substantial 	Final	0	2	1
Business Rates	Substantial 	Substantial 	Final	0	2	1
Housing and Council Tax Benefits	Full 	Substantial 	Final	0	0	3
Accounts Receivable	Full 	Substantial 	Final	0	1	2
Housing Rents	Substantial 	Substantial 	Final	0	4	1
Property	Substantial 	Substantial 	Final	0	3	3





Project	Evaluation Assessment	Testing Assessment	Status	Priority		
				1	2	3
Partnerships	Substantial 	Limited 	Final	1	6	1
Human Resources	Substantial 	Substantial 	Final	0	6	0
Data Quality	Substantial 	Substantial 	Final	0	5	0
Project Management (Transformation)	Limited 	Limited 	Draft	7	8	0
Waste Recycling	Full 	Substantial 	Final	0	3	3
Business Continuity and Disaster Recovery	Substantial 	Limited 	Final	0	7	1
Information Security	Limited 	Limited 	Final	5	15	4
Housing IT System	Substantial 	Substantial 	Draft	0	5	1

Project	Evaluation Assessment	Testing Assessment	Status	Priority		
				1	2	3
Housing Repairs and Maintenance	Substantial 	Substantial 	Final	0	6	2
Housing Asset Management	Substantial 	Substantial 	Final	0	4	0
Planning Fees	Full 	Substantial 	Final	0	7	0
Property Lettings	Substantial 	Substantial 	Final	0	5	0
Total Number of Recommendations				13	107	31

Appendix 3- Key to Assurance Levels

Assurance Gradings

We have four categories by which we classify internal audit assurance over the processes we examine, and these are defined as follows:

Level	Symbol	Evaluation Assessment	Testing Assessment
Full		There is a sound system of internal control designed to achieve the system objectives.	The controls are being consistently applied.
Substantial		Whilst there is a basically sound system of internal control design, there are weaknesses in design which may place some of the system objectives at risk.	There is evidence that the level of non-compliance with some of the controls may put some of the system objectives at risk.
Limited		Weaknesses in the system of internal control design are such as to put the system objectives at risk.	The level of non-compliance puts the system objectives at risk.
Nil		Control is generally weak leaving the system open to significant error or abuse.	Significant non-compliance with basic controls leaves the system open to error or abuse.

The assurance gradings provided above are not comparable with the International Standard on Assurance Engagements (ISAE 3000) issued by the International Audit and Assurance Standards Board and as such the grading of 'Full Assurance' does not imply that there are no risks to the stated objectives.

Recommendation Gradings

In order to assist management in using our internal audit reports, we categorise our recommendations according to their level of priority as follows:

Priority Level	Staff Consulted
1	Major issues for the attention of senior management and the audit committee.
2	Important issues to be addressed by management in their areas of responsibility
3	Minor issues resolved on site with local management.

Appendix 4 - Statement of Responsibility

We take responsibility for this report which is prepared on the basis of the limitations set out below.

The matters raised in this report are only those which came to our attention during the course of our internal audit work and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. Recommendations for improvements should be assessed by you for their full impact before they are implemented. The performance of internal audit work is not and should not be taken as a substitute for management's responsibilities for the application of sound management practices. We emphasise that the responsibility for a sound system of internal controls and the prevention and detection of fraud and other irregularities rests with management and work performed by internal audit should not be relied upon to identify all strengths and weaknesses in internal controls, nor relied upon to identify all circumstances of fraud or irregularity. Auditors, in conducting their work, are required to have regards to the possibility of fraud or irregularities. Even sound systems of internal control can only provide reasonable and not absolute assurance and may not be proof against collusive fraud. Internal audit procedures are designed to focus on areas as identified by management as being of greatest risk and significance and as such we rely on management to provide us full access to their accounting records and transactions for the purposes of our audit work and to ensure the authenticity of these documents. Effective and timely implementation of our recommendations by management is important for the maintenance of a reliable internal control system. The assurance level awarded in our internal audit report is not comparable with the International Standard on Assurance Engagements (ISAE 3000) issued by the International Audit and Assurance Standards Board.

Deloitte & Touche Public Sector Internal Audit Limited St Albans April 2012

In this document references to Deloitte are references to Deloitte & Touche Public Sector Internal Audit Limited.

Registered office: Hill House, 1 Little New Street, London EC4A 3TR, United Kingdom. Registered in England and Wales No 4585162.

Deloitte & Touche Public Sector Internal Audit Limited is a subsidiary of Deloitte LLP, the United Kingdom member firm of Deloitte Touche Tohmatsu Limited ("DTTL"), a UK private company limited by guarantee, whose member firms are legally separate and independent entities. Please see www.deloitte.co.uk/about for a detailed description of the legal structure of DTTL and its member firms.

Member of Deloitte Touche Tohmatsu Limited