Date: October 2010

To: Jane West (Director Finance and Corporate Services) and Mike Sloniowski (Principal Consultant Risk Management)

From: Deloitte and Touche Public Sector Internal Audit Ltd.

Subject: Risk Management – BSI Standard Gap Analysis

Dear Jane and Mike,

1. Introduction

1.1. As part of the 2010/11 Internal Audit Plan approved by the Audit Committee on 23 March 2010, we have undertaken a gap analysis against the BSI Standard for Risk Management (BS31100). This gap analysis is intended to form part of a four year rolling programme under which compliance with the BSI Standard is assessed.

Our audit work was limited to the following two parts of the Standard:

- BSI Standard (Draft) 4.7 – Risk and Impact Categorisation and Measurement
- BSI Standard (Draft) 5.3.2 – Risk Analysis

Further details on these two parts of the Standard can be found in Section 5 of this management letter (Detailed Gap Analysis).

1.2. We are not providing an assurance opinion in respect of our work; however, there are some areas where we have identified gaps between the BS31100 Risk Management Standard and current practices in place across the Council. Where relevant, we have raised recommendations for consideration by management in Section 6 of this management letter.

2. Background

2.1. BSI Standard 31100 was published by the British Standards Institute and came into effect on 31 October 2008. It was drafted to be consistent with the general guidance on risk management given by ISO 31000 but also recognising the knowledge contained in HM Treasury's Orange Book, the Office of Government Commerce publication, "Management of risk: Guidance for practitioners", "Enterprise Risk Management – Integrated Framework and application techniques published by the Committee of Sponsoring Organisations of the Treadway Commission (COSO), and the Risk Management Standard developed by the Institute of Risk Management (IRM), The Association of Insurance and Risk Managers (AIRMIC) and ALARM.

2.2. The Standard provides a guide to risk management principles, models, framework and processes. Its purpose is to assist organisations in achieving their objectives through effective risk management. Effective risk management can assist organisations to achieve their objectives by:

- Reducing the likelihood of events that would have a negative consequence overall and reducing the negative consequences of such events;
- Increasing the likelihood of events that would have a positive consequence overall and increasing the positive consequences of such events;
- Identifying opportunities where taking risks might benefit the organisation;
- Improving accountability, decision making, transparency and visibility;
- Identifying, understanding and managing multiple and cross-organisation risks;
- Executing change more effectively and efficiently and improving project management;
- Providing better understanding of, and compliance with, relevant governance, legal and regulatory requirements, and corporate social responsibility and ethical requirements;
- Protecting revenue and enhancing value for money;
- Protecting reputation and stakeholder confidence;
- Proactively managing the organisation's operations;
- Targeting control expenditure and delivering a cost-optimal control environment;
- Retaining and developing customers through reducing risks to service delivery and enhancing service provision; and
- Making the organisation more flexible and responsive to market fluctuations so that it is better able to satisfy customers' ever changing needs in a continually evolving business environment.

3. Audit Approach and Summary of Findings

3.1. The requirements of BS31100 (draft paragraphs 4.7 and 5.3.2) were compared to the Council's risk management framework, as described in the Risk Management Standard and Policy 2008-2011 and other relevant documents. During our initial meeting with the Principal Consultant, Risk Management we were provided with a copy of the draft version of the Standard and this version was used for the purpose of this exercise. Although no significant differences were noted between the draft and final versions of the Standard, we would recommend that the final version is used for any future exercises.

3.2. In addition, a sample of five departments was visited and interviews were held with relevant officers in order to determine how the requirements of the Standard are applied at an operational level. In relation to paragraph 5.3.2 of the Standard, we attempted to assess a sample of risks from the departments against the requirements of the Standard. Where this was not possible, we examined the types of documented risk information produced and our findings are presented in Section 4 below. Overall, we identified that qualitative and quantitative information on risks is available but there is no explicit link to the risk assessment of service risks identified and included in the service risk registers.

3.3. In the Standard, the word "should" is used to express the recommendations with which users have to comply in order to comply with the Standard. The word "may" is used to express permissibility, e.g. as an alternative to the primary recommendation of the clause. The word "can" is used to express possibility, e.g. a consequence of an action or an event. The specific paragraphs covered in this exercise included provisions mainly introduced with "should" and some with "may" but for the purposes of our analysis they have all been treated as compulsory.

3.4. A line by line presentation of our gap analysis is presented in Section 5. No significant gaps where identified, although consideration should be given to updating the risk register template to include the main impact category and a description of potential consequences. At an operational level, we identified that some teams do not use the risk register template provided and as a result, the risk category is not always identified. Furthermore, the risk analysis is not consistently linked to information produced during the normal course of business. Details of the recommendations raised can be found in Section 6 of this management letter.

4. Risk Information

4.1. Finance

Information produced in the finance department is based on information submitted by departmental finance teams. It is used to complete the monthly CRM report, which is discussed with EMT and also presented to Cabinet. The report presents the overall financial position of the Council and includes details for all individual departments showing their projections for the year. A specific part of the report template submitted by departmental management teams requires them to report on risks and quantify them to show lower and upper limits of the potential financial impact. This information can potentially inform analysis of risks included in the service risk registers and provide quantitative information to assess the risk consequence score.

4.2. Treasury Management

Risk information produced by the Treasury Management Team is mainly determined by relevant legislation and good practice guidance (CIPFA Treasury Management Code of Practice). The Treasury Management Strategy is approved by Cabinet at the beginning of the financial year and includes approved institutions and types of investments as well as limits for the specific investments (prudential indicators). The methodology used to determine acceptable investment counterparties is essentially an assessment of the credit risk associated with the specific institutions. Consideration is also given to liquidity and other relevant risks, which are managed as part of the day to day dealing.

4.3. Information Security

A policy for reporting, assessing and recording information security breaches and information security risks has been developed and it is available on the intranet. In accordance with the Policy, any incidents are assigned a priority rating. This is reviewed by the Information Manager and reported to the IT Strategic Operations Group (ITSOG) on a monthly basis. A log of all incidents is maintained and reported risks are assessed using a template risk register which is based on the corporate one and has been developed with the help of the Principal Consultant, Risk Management. Action taken to deal with incidents and address reported risks is recorded on the incidents/risks log and a RAG system is used to report on status. These risks are not normally linked to the formal risk management process, as they usually relate to a more operational level. Incidents and risks are communicated through the ITSOG and where applicable, messages are sent to staff through e-mail and/or intranet messages.

Information security breaches data can be used to identify and quantify (for instance, through loss experience information) relevant risks and controls for the IT Team and other departments experiencing the breaches and relevant consequences. Consolidated data from the breaches and risk logs can inform the relevant risk assessment in the service risk registers.

4.4. Emergency Planning and Business Continuity

Hammersmith and Fulham is a member of the West London Local Resilience Forum, which also includes Brent, Ealing, Hounslow, Harrow and Hillingdon. The Local Resilience Forum brings together representatives from local authorities, emergency services, government agencies, health, utilities, voluntary organisations, business and the military in order to identify and assess local risks that could cause an emergency so that they can be monitored and managed. A Community Risk Register has been produced. A relevant risk register specific to Hammersmith and Fulham is not in place, however we were informed that the Team is in the process of producing one.

As far as business continuity is concerned, a joint Service Resilience Policy between the Council and NHSHF was recently produced and approved. Services are assessed as critical, key and tertiary in accordance with impact assessment guidelines included in the Policy. Services are not required to identify key risks but a sample of scenarios to consider has been developed, reflecting key risks to service delivery continuity. Specific risks are not currently identified and the links between risk management and business continuity are not mentioned in the Service Resilience Policy and the Risk Management Standard and Policy. We were however informed that there is regular communication between the two services (Business Continuity and Risk Management).

4.5. Fraud Incidents

All referrals received in the fraud service are risk assessed against a set of criteria. The criteria are mainly used for high volume referrals (such as benefit fraud). We were informed that the criteria are reviewed on a regular basis and they are mainly used in order to prioritise resources and manage officers' workload. Information on actual fraud cases investigated is included in a number of SLA reports produced for key stakeholders, including general corporate anti-fraud cases. In addition, quarterly reports are submitted to the Audit and Pensions Committee. These communication arrangements can help relevant departments identify and address significant fraud risk.

Moreover, a fraud risk profiling exercise was completed in 2008. The resulting fraud risk register informs any proactive fraud work undertaken by the Team.

5. Detailed Gap Analysis

Draft BS31100 Provision	Final BS31100 Provision	Risk Management Framework	Practical Application
Paragraph 4.7 – Risk and Impact Categorisation and Measurement			
The organisation should clearly set and document its risk and impact categories and its risk measurement criteria, and integrate these into the components of the risk management framework; applying them each time the risk management process is undertaken.	The organisation should set and document its risk and risk consequence categories and risk criteria, and integrate these into the risk management framework.	Examples of risk categories are included in the Risk Management Standard and Policy. This covers strategic and operational risk categories. Risk impact categories are included in the guides/tables provided to support the classification of risk impacts. Risk criteria are established in the Risk Management Standard and Policy.	The template risk register included in the Risk Strategy requires the identification of the risk category. A sample of five services was visited and the relevant risk registers were obtained. Risk categories had only been identified in one case. Risks are assessed in terms of impact and likelihood but the relevant impact category (or the main one) is not identified in the risk registers. **See Recommendations 6.1 & 6.2.**
The organisation should review its risk and impact categorisations and its risk measurement criteria to ensure they remain fit for purpose.	N/A – not explicitly included in the final version	The risk and impact categories and risk criteria are reviewed when the Risk Management Standard and Policy is reviewed. This covers a period of three years and was last reviewed in 2008.	N/A

Draft BS31100 Provision	Final BS31100 Provision	Risk Management Framework	Practical Application
The number and type of risk categories that an organisation employs, and the level of granularity within categories, should suit the size, purpose, nature, complexity and environment in which the organisation operates, and reflect the maturity of risk management within it. While risk categories differ between organisations, risk categories in common usage include: • Market Risk; • Credit Risk; • Operational Risk; • Project Risk; • Financial Risk; • Strategic Risk; and • Reputational Risk. Risk categories can be influenced by legal and regulatory requirements or sector practice.	The organisation should develop risk categories that suit its size, purpose, nature, complexity and context, while taking into account the maturity of its risk management.	Risk categories, risk consequence categories and risk criteria are included in the Risk Management Standard and Policy. Approval by an appropriate body can help to ensure that they are suitable for the organisation. We examined the minutes of Audit Committee meetings for 2008 and 2009 and there was no evidence of the Risk Management Standard and Policy being approved. **See Recommendation 6.5.**	N/A
The purpose of categorisation of impacts is to allow consistent assessment, profiling and reporting of the effects/consequences of actual and potential events, and to facilitate comparison across the	To allow consistent assessment, profiling and reporting of the consequences of actual and potential events, and to facilitate comparison across the organisation, the organisation should develop risk consequence	Risk consequence categories are described in a number of tables included in the Risk Management Standard and Policy, designed to assist with the assessment of potential impact of indentified	The risk registers used do not record the main impact category for identified risks. **See Recommendation 6.1.**

Draft BS31100 Provision	Final BS31100 Provision	Risk Management Framework	Practical Application
organisation. While impact categories differ between organisations, impact categories in common usage include: - Financial; - People; - Service; - Clients; - Stakeholders; - Investors/funders; - Production; - Legal and compliance; and - Reputation and Brand. The number and type of impact categories that an organisation employs should suit its size, purpose, nature, complexity and environment in which the organisation operates, and reflect the maturity of risk management within it. The organisation should have both financial and non-financial impact categories.	categories that suit its size, purpose, nature, complexity and context, while taking into account the maturity of its risk management capability.	risks.	

Draft BS31100 Provision	Final BS31100 Provision	Risk Management Framework	Practical Application
The organisation should develop risk measurement criteria against which the risk can be consistently assessed. A basic approach is to consider the two dimensions of: • Likelihood; and • Impact (financial and non-financial).	To enable risks to be consistently assessed, the organisation should develop risk criteria that suit its size, purpose, nature, complexity, management level and context, while taking into account the maturity of its risk management. A basic approach is to consider likelihood and consequence and the time period over which consequences are assessed.	Risk measurement criteria have been developed and are included in the Risk Management Standard and Policy. However, the time period over which consequences are assessed is not referred to in the Policy. **See Recommendation 6.6.**	All risks in the risk registers are assessed in terms of impact and likelihood.
Measurement criteria need to be calibrated. For the basic approach, the organisation would need to define for each dimension the scale to be used, e.g. this could be "low, medium, high", or a scale of 1 to 5, and the criteria for each element of the scale, e.g. for impact, "High" may equate to greater than a £10m loss.	N/A – not covered in the final version	Guidelines regarding measurement criteria are included in the Risk Management Standard and Policy.	N/A

Draft BS31100 Provision	Final BS31100 Provision	Risk Management Framework	Practical Application
Risk measurement criteria should take into account, and be in keeping with, the risk appetite of the organisation, and should allow for all risks to be measured, including those that do not naturally lend themselves to numerical diagnosis, e.g. reputational risk.	The organisation's risk criteria should take into account its risk appetite and allow for all risks to be measured, including those that do not normally lend themselves to numerical analysis.	Risk criteria, as described in the risk consequence tables, are used to determine the risk score, which is then linked to the risk appetite. However, linkages are not described in the relevant part of the Risk Management Standard and Policy. **See Recommendation 6.4.**	N/A
The criteria should be communicated through the organisation in order for all to share a common understanding of how risk is measured. Tables and matrices can assist.	The risk categories and risk consequence categories should be communicated throughout the organisation in order for all to share a common understanding. The criteria should be communicated throughout the organisation in order for all to share a common understanding of how risk is measured.	The criteria are communicated in the Risk Management Standard and Policy and tables are used to describe the different levels of potential risk consequences. The Risk Management Standard and Policy is available to staff through the intranet.	N/A

Draft BS31100 Provision	Final BS31100 Provision	Risk Management Framework	Practical Application
Paragraph 5.3.2 – Risk Analysis			
The likelihood of each risk occurring and its impact should be determined, taking into account existing controls and their adequacy and effectiveness. This activity should be undertaken in accordance with the risk measurement criteria set out in the risk management framework to help ensure consistency of analysis and aid the comparison and prioritisation of risks.	Each risk should be analysed to an appropriate extent, considering its consequences, and summarised in terms of the consequences arising and their likelihood.	Risk criteria (impact and likelihood) are described in the Risk Management Standard and Policy.	A sample of five services was visited, the risk registers were obtained and the risks relevant to the services were examined. Risks in the risk registers had been scored in terms of impact and likelihood but these had not been described in detail. There was no documentation or relevant evidence supporting the scores assigned. **See Recommendation 6.1.**

Draft BS31100 Provision	Final BS31100 Provision	Risk Management Framework	Practical Application
Risk analysis may be undertaken with varying degrees of detail depending upon the risk, the purpose of the analysis, and the information, data and resources available. Analysis may be qualitative, semi-quantitative or quantitative, or a combination of these. In practice, qualitative analysis is often used to first rank the risks in relation to one another, to indicate the level of risk and to reveal the most significant risks. It might subsequently be necessary to undertake more detailed or quantitative analysis of the most significant risks. The complexity and costs of qualitative risk analysis are lower than those of semi-quantitative analysis, which in turn are lower than those of quantitative analysis.	Risk analysis may be undertaken with varying degrees of detail depending upon the risk, the purpose of the analysis, and the information data and resources available. Analysis may be qualitative or quantitative or a combination of these.	There is no detailed guidance on how risk analysis should be undertaken. **See Recommendation 6.3.**	In all areas visited, we could not see any evidence of qualitative risk analysis (for the relevant risks in the service risk registers).

Draft BS31100 Provision	Final BS31100 Provision	Risk Management Framework	Practical Application
Risk analysis is an iterative process, being repeated as more data become available, e.g. as a project evolves and develops. Impacts may be determined by modelling the outcomes of an event of set of events, or by extrapolation from experimental studies or past data. There are many tools for presenting and communicating the results of risk analysis; some examples are provided by the standard.	Risk analysis should be an iterative process, being repeated as more data become available. It may take into account the inherent risk, the controls in place and how well these mitigate the risk, and be undertaken in accordance with the risk criteria.	The Risk Management Standard and Policy suggests that departmental risk registers should be reviewed at least quarterly. This should ensure that risks are re-assessed regularly.	We were informed during our meetings with the five services visited that risk registers are reviewed at least quarterly. This process is monitored by the Principal Consultant, Risk Management. We examined current and older versions of the risk registers for the services visited and we could see evidence of iterations and updates of the risk register. For three of the areas visited we were informed that risk registers are produced during “brainstorming” sessions. No information could be provided for the other two areas visited as the officers interviewed were not directly involved in the process. Please note that detailed testing regarding the updates of risk registers (and compliance with the quarterly requirement included in the Policy) was not undertaken as this will be covered in other risk management audits planned to be completed later in the year.

Draft BS31100 Provision	Final BS31100 Provision	Risk Management Framework	Practical Application
Once all risk have been analysed, and the level of risk has been established for each risk, a prioritised list of risks should be produced. As well as the likelihood of occurrence and scale of impact, analysis criteria may include proximity and timing.	N/A – not covered in the final version	A paragraph has been included in the Risk Management Standard and Policy regarding risk prioritisation and escalation. Proximity and timing of risks are not explicitly mentioned. The time horizon of the risk is mentioned in a guidance document on completing the risk section of Cabinet reports. Although this is an optional part of the Standard, consideration should be given to including relevant guidance in the Risk Management Standard and Policy. **See Recommendation 6.6.**	As it is not covered in the main risk management guidance, proximity and timing of risks had not been explicitly described for any of the services visited or risk registers examined. Even though risks had not been re-arranged in any specific order, the final score for all risks had been calculated and this can serve as prioritisation.

6. Recommendations

6.1. Risk Consequence Category and Description

BS31100 Provision	Issue	Recommendation
The organisation should set and document its risk and risk consequence categories and risk criteria, and integrate these into the risk management framework.	Risk and risk consequence categories and risk criteria are included in the Risk Management Standard and Policy. However, risk consequence categories are not identified and described in the risk registers as the template risk register does not include relevant columns.	The template risk register included in the Risk Management Standard and Policy should be updated to include a column showing the main risk consequence category associated with the identified risk and a description of the potential risk consequence. Potential consequences should be linked to the impact guide and the template risk register should be amended to facilitate this.
Management Response	**Responsible Officer**	**Deadline**
Agreed	Principal Consultant Risk Management	March 2011

6.2. Use of Template Risk Register

BS31100 Provision	Issue	Recommendation
The organisation should set and document its risk and risk consequence categories and risk criteria, and integrate these into the risk management framework.	Risk categories are described in the Risk Management Standard and Policy and a specific column has been included in the template risk register. Risk categories had only been identified in one out of four risk registers examined. Two risk registers were not completed using the suggested template.	Services across the Council should be reminded to use the template risk register included in the Risk Management Standard and Policy so that all required information is captured. Where the template is not understood, support and additional training should be provided as required.
Management Response	**Responsible Officer**	**Deadline**
Agreed	Principal Consultant Risk Management	March 2011

6.3. Risk Analysis Tools and Guidance

BS31100 Provision	Issue	Recommendation
Risk analysis may be undertaken with varying degrees of detail depending upon the risk, the purpose of the analysis, and the information data and resources available. Analysis may be qualitative or quantitative or a combination of these.	There is no detailed guidance on how risk analysis should be undertaken. In all five areas visited, we could not see any evidence of qualitative risk analysis (for the risks relevant to the risk registers).	The Risk Management Standard and Policy should be amended to include guidance on risk analysis and a list of potential tools that can be used for risk identification, analysis and reporting purposes. Services across the Council should be instructed to link the risk analysis process to quantitative and qualitative information on potential risks produced in the normal course of business, where applicable.
Management Response	**Responsible Officer**	**Deadline**
Agreed	Principal Consultant Risk Management	March 2011

6.4. Risk Appetite

BS31100 Provision	Issue	Recommendation
The organisation's risk criteria should take into account its risk appetite and allow for all risks to be measured, including those that do not normally lend themselves to numerical analysis.	Risk criteria, as included in the risk consequence tables, are used to determine the risk score, which is then linked to the risk appetite. However, the connection is not clear in the Risk Management Standard and Policy.	The Council's risk appetite should be clearly defined in the Risk Management Standard and Policy. This should be linked to the risk impact/magnitude tables. Consideration should be given to simplifying the risk impact/magnitude tables and consolidating them into one overall table. A potential example has been included for information in Appendix 1.
Management Response	**Responsible Officer**	**Deadline**
Agreed	Principal Consultant Risk Management	March 2011

6.5. Risk Management Standard and Policy Approval and Review

BS31100 Provision	Issue	Recommendation
The organisation should develop risk categories, risk consequence categories and risk criteria that suit its size, purpose, nature, complexity and context, while taking into account the maturity of its risk management.	Risk categories, risk consequence categories and risk criteria are included in the Risk Management Standard and Policy. Approval by an appropriate body can help to ensure that they are suitable for the organisation. We examined the minutes of Audit Committee meetings for 2008 and 2009 and there was no evidence of the Risk Management Standard and Policy being approved.	The Risk Management Standard and Policy should be formally approved by the Audit and Pensions Committee and evidenced as such e.g. within the meeting minutes. Consideration should be given to reviewing the Policy on an annual basis to ensure risk management objectives and the Council's risk appetite remains relevant to the external and internal environment.
Management Response	**Responsible Officer**	**Deadline**
Agreed	Principal Consultant Risk Management	March 2011

6.6. Proximity and Timing of Identified Risks

BS31100 Provision	Issue	Recommendation
To enable risks to be consistently assessed, the organisation should develop risk criteria that suit its size, purpose, nature, complexity, management level and context, while taking into account the maturity of its risk management. A basic approach is to consider likelihood and consequence and the time period over which consequences are assessed. Once all risk have been analysed, and the level of risk has been established for each risk, a prioritised list of risks should be produced. As well as the likelihood of occurrence and scale of impact, analysis criteria may include proximity and timing [Draft Version of the Standard].	The proximity and timing of risks are not explicitly referred to in the Risk Management Standard and Policy or recorded in the risk registers. Also the time period over which consequences should be assessed is not mentioned.	Consideration should be given to explicitly documenting in the risk registers the proximity and timing of identified risks as well as the time period over which risk consequences are assessed. Relevant guidelines should be included in the Risk Management Standard and Policy.
Management Response	**Responsible Officer**	**Deadline**
Agreed	Principal Consultant Risk Management	March 2011

Appendix 1 – Example of Consolidated Risk Impact/Magnitude Guide

Impact Description	Category	Description
1 Very Low	Cost/Budgetary Impact	£0 to £25,000
	Impact on life	Temporary disability or slight injury or illness less than 4 weeks (internal) or affecting 0-10 people (external)
	Environment	Minor short term damage to local area of work.
	Reputation	Decrease in perception of service internally only – no local media attention
	Service Delivery	Failure to meet individual operational target – Integrity of data is corrupt no significant effect
2 Low	Cost/Budgetary Impact	£25,001 to £100,000
	Impact on life	Temporary disability or slight injury or illness greater than 4 weeks recovery (internal) or greater than 10 people (external)
	Environment	Damage contained to immediate area of operation, road, area of park single building, short term harm to the immediate ecology or community
	Reputation	Localised decrease in perception within service area – limited local media attention, short term recovery
	Service Delivery	Failure to meet a series of operational targets – adverse local appraisals – Integrity of data is corrupt, negligible effect on indicator
3 Medium	Cost/Budgetary Impact	£100,001 to £400,000
	Impact on life	Permanent disability or injury or illness
	Environment	Damage contained to Ward or area inside the borough with medium term effect to immediate ecology or community
	Reputation	Decrease in perception of public standing at Local Level – media attention highlights failure and is front page news, short to medium term recovery
	Service Delivery	Failure to meet a critical target – impact on an individual performance indicator – adverse internal audit report prompting timed improvement/action plan - Integrity of data is corrupt, data falsely inflates or reduces outturn of indicator
4 High	Cost/Budgetary Impact	£400,001 to £800,000
	Impact on life	Individual Fatality
	Environment	Borough wide damage with medium or long term effect to local ecology or community
	Reputation	Decrease in perception of public standing at Regional level – regional media coverage, medium term recovery

Impact Description	Category	Description
	Service Delivery	Failure to meet a series of critical targets – impact on a number of performance indicators – adverse external audit report prompting immediate action - Integrity of data is corrupt, data falsely inflates or reduces outturn on a range of indicators
5 Very High	Cost/Budgetary Impact	£800,001 and over
	Impact on life	Mass Fatalities
	Environment	Major harm with long term effect to regional ecology or community
	Reputation	Decrease in perception of public standing nationally and at Central Government – national media coverage, long term recovery
	Service Delivery	Failure to meet a majority of local and national performance indicators – possibility of intervention/special measures – Integrity of data is corrupt over a long period, data falsely inflates or reduces outturn on a range of indicators

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
London
October 2010

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