

RSM! Tenon



SOUTH CAMBRIDGESHIRE DISTRICT COUNCIL

Internal Audit Progress Report

Corporate Governance Committee Meeting: March 2011

RSM! Tenon

CONTENTS

Section		Page
1	Introduction	1
2	Final reports issued	1
3	Key Findings from Internal Audit Work	1
4	Work in Progress or Planned	1
5	Liaison with Management and External Audit	2
6	Changes to our Plan	2
7	Client Briefings	3
Appendices		
A	2010/11 Work Completed to Date Including Summary of Assurance Levels and Recommendations	4
B	Work in Progress or Yet to Start (including reports still in draft)	9
C	Client Briefings	10

The matters raised in this report are only those which came to our attention during our internal audit work and are not necessarily a comprehensive statement of all the weaknesses that exist, or of all the improvements that may be required. Whilst every care has been taken to ensure that the information provided in this report is as accurate as possible, based on the information provided and documentation reviewed, no complete guarantee or warranty can be given with regard to the advice and information contained herein. Our work does not provide absolute assurance that material errors, loss or fraud do not exist.

This report is prepared solely for the use of South Cambridgeshire District Council. Details may be made available to specified external agencies, including external auditors, but otherwise the report should not be quoted or referred to in whole or in part without prior consent. No responsibility to any third party is accepted as the report has not been prepared, and is not intended for any other purpose.

© 2010 RSM Tenon Limited

RSM Tenon Limited is a member of RSM Tenon Group

RSM Tenon Limited is an independent member firm of RSM International an affiliation of independent accounting and consulting firms. RSM International is the name given to a network of independent accounting and consulting firms each of which practices in its own right. RSM International does not exist in any jurisdiction as a separate legal entity.

RSM Tenon Limited (No 4066924) is registered in England and Wales. Registered Office 66 Chiltern Street, London W1U 4GB. England

1. INTRODUCTION

1.1 The periodic internal audit plan for 2010/11 was approved by the Corporate Governance Committee on 31 March 2010. This report summarises the outcome of work completed to date against that plan. Appendices A and B provide cumulative data in support of internal audit performance.

2. FINAL REPORTS ISSUED

2.1 We have finalised the following reports since the last Committee meeting; these are in the areas of:

- NNDR (11.10/11);
- Financial Planning and Budgetary Control (17.10/11);
- Risk Management and Assurance Stocktake (19.10/11);
- Safeguarding (21.10/11);
- Reconciliations (22.10/11);
- Follow Up GCSX CoCo Annual Assessment (23.10/11);
- Planning (24.10/11);
- Housing Benefits (25.10/11);
- Corporate Governance (26.10/11); and
- Follow Up HR Absence Management (29.10/11).

2.2 Appendix A summarises our opinions and the number of recommendations made during the year to date.

3. KEY FINDINGS FROM INTERNAL AUDIT WORK

3.1 The Corporate Governance Committee should note that the assurances given in our audit assignments will be taken into account when we form our overall opinion on the assurance that we can provide in our Annual Report at the end of the year. In particular the Corporate Governance Committee should note that any negative assurance opinions will need to be noted in the annual report and may result in a qualified or negative annual opinion.

3.2 No common weaknesses have been identified within our reports.

4. WORK IN PROGRESS OR PLANNED

4.1 We have issued further draft reports since the last Committee meeting; these are in the areas of:

- Capital Expenditure and Asset Management (20.10/11);
- Environmental Health – Health and Safety (27.10/11);
- Follow Up – Health and Safety and Electrical Safety Programme (28.10/11); and
- Follow Up (30.10/11).

4.2 We are currently at the fieldwork stage of the following review:

- Top Up Testing; and
- Annual Governance Statement.

5. LIAISON WITH MANAGEMENT AND EXTERNAL AUDIT

5.1 Since the last Corporate Governance Committee we have met with Management and the Audit Commission and we have developed a detailed protocol setting out the respective roles and working practices for the key financial controls including the areas to be covered and sample sizes during both are main testing and the top up testing at the year end.

6. CHANGES TO OUR PLAN

6.1 Changes reported previously:

- Due to the current tendering exercise of the Responsive Repairs function, we revised the Housing Responsive Repairs Review to be a follow up of the previous recommendations only instead of the planned review, this has reduced the resources required to complete this review.
- We added Top Up Testing to the Internal Audit Plan (in line with the agreed audit protocol identified above) to provide assurance to management and the Audit Commission on compliance of key financial controls between the completion of the main audit fieldwork and the year end.
- The reconciliations work has been added to accommodate the requirements of External Audit.
- We have undertaken a review of data submitted by MRUK relating to National Indicator 182 (Satisfaction of business with local authority regulation services) for the year 2009/10. A memo summarising the outcomes of this have been reported to management.

- We have undertaken a review of the Redundancy process undertaken within the Council.

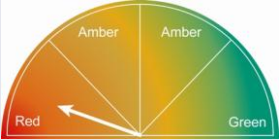
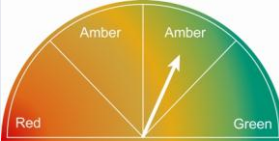
6.2 In addition, at the request of management, we have cancelled the Contact Centre Review and Performance Management and added to the audit plan reviews of HR Follow Up and Health and Safety – Electrical Safety Follow Up have been added to the audit plan.

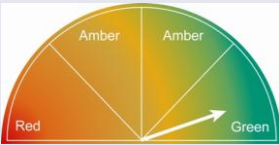
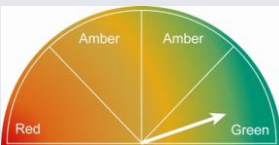
7. CLIENT BRIEFINGS

7.1 There have been three relevant client briefing issued since the last Corporate Governance Committee, further details of these can be found at Appendix C of our report.

APPENDIX A: 2010/11 WORK COMPLETED TO DATE INCLUDING SUMMARY OF ASSURANCE LEVELS AND RECOMMENDATIONS

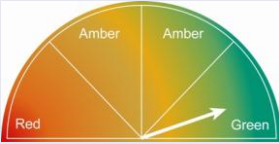
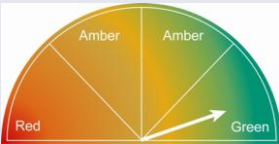
Reports being considered at this Committee are shown in italics.

Auditable Area	Start Date	Debrief date	Draft report issued	Responses received	Final report issued	Corporate Governance Committee	Assurance level given	Number of Recommendations Made				
								Actual (Planned)	High	Medium	Low	In Total
Health and Safety – Tenant Electrical Safety Programme (1.10/11)	14/04/10	16/04/10	07/05/10	16/06/10	16/06/10	June 2010		3	2	7	12	12
HR Absence Management (2.10/11)	18/05/10	27/05/10	04/06/10	10/06/10	14/06/10	June 2010		0	3	2	5	5
Housing Maintenance – Planned and Cyclical (3.10/11)	24/05/10	28/05/10	16/06/10	21/06/10	21/06/10	Sept 2010		0	3	3	6	6
Housing Responsive Repairs Follow Up (4.10/11)	01/07/10	05/07/10	19/07/10	27/07/10	28/07/10	Sept 2010	Follow Up – Little Progress	0	2	5	7	7
HR – Redundancies (5.10/11)	23/08/10	26/08/10	06/09/10 20/09/10	17/09/10	29/09/10 26/10/10	Jan 2011	Advisory	-	-	-	13	13

Auditable Area	Start Date	Debrief date	Draft report issued	Responses received	Final report issued	Corporate Governance Committee	Assurance level given	Number of Recommendations Made				
								High	Medium	Low	In Total	Agreed
Homelessness and Housing Advice (6.10/11)	25/08/10	02/09/10	14/09/10	16/09/10	16/09/10	Jan 2011		0	0	11	11	11
Section 106 (7.10/11)	01/09/10	07/09/10	30/09/10	16/11/10	16/11/10	Jan 2011		0	1	1	2	2
Asset Management (Housing) (8.10/11)	23/09/10	28/09/10	12/10/10	15/12/10	16/12/10	Jan 2011		0	2	1	3	3
General Ledger (9.10/11)	27/9/10	1/10/10	13/10/10	21/12/10	21/12/10	Jan 2011		0	0	1	1	1
Payroll (10.10/11)	4/10/10	13/10/10	22/10/10	6/12/10	6/12/10	Jan 2011		0	0	1	1	1
NNDR (11.10/11)	04/10/10	14/10/10	22/10/10	14/1/11	14/1/11	March 2011		0	4	3	7	7

Auditable Area	Start Date	Debrief date	Draft report issued	Responses received	Final report issued	Corporate Governance Committee	Assurance level given	Number of Recommendations Made				
								High	Medium	Low	In Total	Agreed
Income and Debtors (12.10/11)	11/10/10	15/10/10	27/10/10	22/12/10	22/12/10	Jan 2011		0	0	1	1	1
Procurement (13.10/11)	8/10/10	15/10/10	27/10/10	12/11/10	12/11/10	Jan 2011		0	0	2	2	2
Housing Rents (14.10/11)	23/09/10	14/10/10	27/10/10	05/11/10	05/11/10	Jan 2011		0	0	4	4	4
Council Tax (15.10/11)	11/10/10	18/10/10	2/11/10	21/12/10	21/12/10	Jan 2011		0	2	2	4	4
Cash, Banking and Treasury Management (16.10/11)	19/10/10	21/10/10	2/11/10	21/12/10	21/12/10	Jan 2011		0	0	2	2	2
Financial Planning and Budgetary Control (17.10/11)	01/11/10	10/11/10	25/11/10	24/12/10	4/1/11	March 2011		0	1	1	2	2

Auditable Area	Start Date	Debrief date	Draft report issued	Responses received	Final report issued	Corporate Governance Committee	Assurance level given	Number of Recommendations Made				
								High	Medium	Low	In Total	Agreed
Payment and Creditors (18.10/11)	22/11/10	25/11/10	30/11/10	23/12/10	23/12/10	Jan 2011		0	1	4	5	5
Risk Management and Assurance Stocktake (19.10/11)	25/08/10	29/11/10	07/12/10 16/2/11	8/2/11	3/3/11	March 2011	ADVISORY	1	1	5	7	7
Safeguarding (21.10/11)	16/11/10	08/12/10	10/02/11	14/03/11	18/03/11	March 2011		0	2	7	9	9
Reconciliations (22.10/11)	November 2010	24/11/10	5/1/11	7/3/11	7/3/11	March 2011		0	1	2	3	3
Follow Up CoCo Assessment (23.10/11); GCSX Annual	November 2011	17/11/10	05/1/11 08/03/11	04/03/11	14/03/11	March 2011		0	7	6	13	12 (1 Low not)
Planning (24.10/11)	13/12/10	17/12/10	12/1/11	27/1/11	27/1/11 3/3/11	March 2011		0	5	6	11	11

Auditable Area	Start Date	Debrief date	Draft report issued	Responses received	Final report issued	Corporate Governance Committee	Assurance level given	Number of Recommendations Made				
								High	Medium	Low	In Total	Agreed
<i>Housing Benefits</i> (25.10/11)	5/01/11	10/1/11	31/1/11	18/2/11	18/2/11	March 2011		0	0	0	0	0
<i>Corporate Governance</i> (26.10/11)	04/02/11	21/1/11	31/1/11 18/2/11	18/2/11 21/2/11	22/2/11	March 2011		0	0	1	1	1
<i>Follow Up – HR Absence Management</i> (29.10/11)	07/02/11	09/02/11	7/3/11	7/3/11	8/3/11	March 2011	ADEQUATE PROGRESS	0	0	2	2	2
Totals to date:								4	37	80	121 + 13	121 + 13

APPENDIX B: WORK IN PROGRESS OR YET TO START (INCLUDING REPORTS STILL IN DRAFT)

Auditable Area	Start Date	Debrief date	Draft report issued
Capital Expenditure and Asset Management (20.10/11)	29/11/10	02/12/10	10/02/11
Environmental Health – Health and Safety (27.10/11)	17/02/11	25/2/11	28/02/11
Follow Up Health and Safety and Electrical Safety Programme (28.10/11)	07/02/11	09/02/11	07/03/11
Follow Up (30.10/11)	08/02/11	14/2/11	07/03/11
Top Up Testing	07/03/11		
Annual Governance Statement	March 2011		
Performance Management	Cancelled		
Contact Centre	Cancelled		
Audit Management	Ongoing		

APPENDIX C: CLIENT BRIEFINGS

The Role of the Head of Internal Audit

31 January 2011

Client Briefing - LGe 01.11

CIPFA STATEMENT ON THE ROLE OF THE HEAD OF INTERNAL AUDIT (HIA)

An internal audit service that is well positioned to provide independent advice and assurance to management is a key element of strong corporate governance in any organisation. Reflecting the importance of internal audit in the public sector, the Chartered Institute of Public Finance and Accountancy (CIPFA) has published its statement on the *Role of the Head of Internal Audit in Public Service Organisations*.

CIPFA's intention is that this document is applicable to all public sector organisations, and although the statement is based and linked to the CIPFA Code of Practice for Internal Audit in Local Government, it is still useful for organisations that must comply with other standards such as the Government Internal Audit Standards, NHS Internal Audit Standards and the International Standards published by the Institute of Internal Auditors.

The Statement was published following consultation, and CIPFA is now consulting on a local government specific version of the document.

This briefing provides an overview of the key messages from the Statement regarding the role of the HIA.

PRINCIPLES FOR THE HIA

The Statement is principles led, and is intended to help clarify the role of the HIA.

The Head of Internal Audit plays a critical role in delivering the organisation's strategic objectives by:

1. championing best practice in governance, objectively assessing the adequacy of governance and management of existing risks, commenting on responses to emerging risks and proposed developments; and
2. giving an objective and evidence based opinion on all aspects of governance, risk management and internal control.

To perform this role the Head of Internal Audit:

3. must be a senior manager with regular and open engagement across the organisation, particularly with the Leadership Team and with the Audit Committee;

4. must lead and direct an internal audit service that is resourced to be fit for purpose; and
5. must be professionally qualified and suitably experienced.

ARRANGEMENTS TO SUPPORT THE PRINCIPLES

CIPFA's statement provides a useful overview of the core elements that must be in place to support achievement of the five principles. These can be categorised as:

- The organisation and its governance requirements;
- Clear core responsibilities for the HIA; and
- Qualities needed for the individual delivering the HIA role.



© CIPFA 2010

USING THE STATEMENT

The Statement is useful for a wider audience than just internal auditors, and we recommend that Audit Committees and senior management consider the content of the Statement and how this applies to their organisation and governance arrangements.

Each public sector organisation is responsible for maintaining sound governance, and therefore as part of this should consider if arrangements in place support the HIA in delivering the optimal service to management.

The full document is available electronically at: <http://www.cipfa.org.uk/roleoftheHIA/>

REVISION OF THE ACCOUNTS AND AUDIT REGULATIONS - CHANGES SPECIFIC TO INTERNAL AUDIT

The Department for Communities and Local Government has published a consultation on amendments to the Accounts and Audit Regulations 2003. The consultation, which is open until 4 March 2011, proposes two changes specific to internal audit:

1. The wording of regulation 6 is amended to remove the reference to **'the system'** of internal audit; and
2. The requirement for organisations to conduct an annual review of internal audit is removed for smaller bodies (i.e. those bodies with gross income or expenditure not exceeding £6.5m per annum).

Delay to Bribery Act Enforcement

3 February 2011

Client Briefing - Gen 01.11

The Ministry of Justice has announced a further delay in the planned enforcement date of the Bribery Act 2010. The Bribery Act was due to be enforceable from April 2011, however on the 31 January 2011 a spokesperson for the Ministry of Justice said:

'We are working on the guidance to make it practical and comprehensive for business. We will come forward with further details in due course. When the guidance is published it will be followed by a three month notice period before implementation of the Act.'

It appears the sticking point is focused in the main around overseas operations and the use of agents. It would be prudent for those businesses that have started to apply anti bribery measures to continue with their implementation to ensure speedy compliance with the Bribery Act 2010 when the revised enforcement date of the Act is made available.

This delay presents businesses who have not taken any action in relation to the Bribery Act 2010 with an opportunity to ensure that anti bribery measures are implemented prior to the revised enforcement date.

RSM Tenon will continue to provide updates, guidance, support and assistance in relation to ensure adequate procedures are addressed in relation to the Bribery Act 2010.

For further information please contact:

Allan Maund Regional Investigations Manager Email: allan.maund@rsmtenon.com Mobile: 07748 152 013	John Baker Director, Fraud Solutions Email: John.baker@rsmtenon.com Mobile: 07753 584 973
--	---

Fines Issued by the Information Commissioner

9 March 2011

Client Briefing - Gen 02.11

The Information Commissioner issues his first fines under new data protection powers and says *“where personal information is involved, password protection for portable devices is simply not enough”*.

FINES ISSUED

Hertfordshire County Council was fined £100,000 in November 2010 for two serious incidents involving the faxing of highly sensitive personal information to the wrong recipients. The second fine to be levied, totalling £60,000, was issued to Sheffield-based employment services company A4e for the loss of an unencrypted laptop which contained personal information relating to 24,000 people who had used community legal advice centres in Hull and Leicester. A4e reported the incident to the Information Commissioner Office (ICO) and subsequently notified those people whose data could have been accessed. The Commissioner ruled that a monetary penalty of £60,000 was appropriate, given that access to the data could have caused substantial distress.

A4e did not take reasonable steps to avoid the loss of data when it issued its employee with an unencrypted laptop, despite knowing the amount and type of data that would be processed on it.

Two further fines followed on the 8 February 2011 of £80,000 and £70,000 to Ealing Council and Hounslow Council respectively. Two laptops containing the details of approximately 1,700 individuals were stolen from the home of an Ealing Council employee. Both laptops were password protected but unencrypted – despite this being in breach of both councils’ policies. Hounslow Council breached the Data Protection Act (the Act) by failing to have a written contract in place with Ealing Council but also failing to monitor Ealing Council’s procedures for operating the data processor service securely.

The announcements of data protection breaches and subsequent fines should alert all businesses to look in depth and consider their compliance arrangements. It is clear, fines for breaching the Act will not solely be levied on the public sector and with a maximum fine of half a million pounds, the Information Commissioner has a strong hand to play.

FORM OF SANCTION

A fine is just one of the non compliance remedies available to the Information Commissioner to attempt to change the behaviour of organisations and individuals that collect, use and keep personal information and they are not mutually exclusive. The Information Commissioner can use them in combination where justified. The main options available to him include:

- Serve information notices requiring organisations to provide the ICO with specified information within a certain time period;
- Issue undertakings committing an organisation to a particular course of action in order to improve its compliance;
- Conduct consensual assessments (audits) to check organisations are complying;
- Issue monetary penalty notices, requiring organisations to pay up to £500,000 for serious breaches of the Data Protection Act occurring on or after 6 April 2010; and
- Prosecute those who commit criminal offences under the Act.

In all cases the actions, where imposed, are published in the public domain and so will have reputation repercussions for the defaulting organisation.

COMMON BREACHES AND MITIGATING ACTION

Whilst Hertfordshire County Council's fine involved unlawful disclosure on two occasions via fax, by far the largest proportion of omissions reported to the Information Commissioner involves the loss of laptops or portable media (CD / USB) containing personal information where the laptop or media drive is not encrypted. In 2010, the Information Commissioner took published action against 50 organisations, 50% of these involved the loss / theft of unencrypted laptops or portable media. A further 25% were to tighten procedures following avoidable unlawful disclosure of personal data and 10% directly related to the lack of data protection training to staff within organisations.

Of the four monetary penalties that have been served so far, three involve the loss of unencrypted laptops. Where personal information is involved, password protection for portable devices is simply not sufficient to meet the requirements of the Information Commissioner. The penalty against Hounslow Council clearly shows that an organisation cannot simply hand over the processing of the personal information it is responsible for to a data processor unless they ensure that the information will be properly protected. This is not just direct processing such as Payroll, but will include any form of external support where a third party has access to your information as a data processor.

Although there is no legal obligation on data controllers to report breaches of security which result in loss, release, or corruption of personal data, the Information Commissioner through guidance issued last year believes serious breaches should be brought to the attention of his Office. An unreported breach is likely to incur a greater penalty should it subsequently be brought to the attention of the Information Commissioner.

All data controllers have a statutory responsibility to comply with the eight principles of the Data Protection Act to ensure data is obtained and processed fairly and lawfully and not processed in any manner incompatible with the purpose for which it was provided and to ensure appropriate and proportionate security of the personal data they hold. Ensuring compliance with the eight principles is not simply an issue of operating within the law; it also requires procedures and controls to be in place for the effective handling of personal information and respecting the interests of data subjects.

The seventh principle of the Act requires that appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data. Whilst there are many measures or controls that an organisation can implement, the two which we consider to be the most pertinent and should be given the highest priority are the encryption of all laptops / mobile and portable computing and the regular awareness training of staff.

- Can you be sure that your data protection and information security procedures are fit for purpose and effective in protecting your organisation from reputation damage, enforcement action and monetary penalty?
- Are your staff adequately trained and aware of their responsibilities?
- Do you know where all of your organisation's personal data is and what it is being used for?

If you cannot take comfort in your answer to any of the above, we can help.

For more information or support please contact: Terry Day on 07788 150 913 or email: terry.day@rsmtenon.com