



Committee: AUDIT COMMITTEE
Date: WEDNESDAY, 21 JANUARY 2015
Venue: MORECAMBE TOWN HALL
Time: 6.00 P.M.

A G E N D A

1. **Apologies for Absence**

2. **Minutes**

Minutes of meeting held on 17 September 2014 (previously circulated).

3. **Items of Urgent Business authorised by the Chairman**

4. **Declarations of Interest**

To receive declarations by Members of interests in respect of items on this Agenda.

Members are reminded that, in accordance with the Localism Act 2011, they are required to declare any disclosable pecuniary interests which have not already been declared in the Council's Register of Interests. (It is a criminal offence not to declare a disclosable pecuniary interest either in the Register or at the meeting.)

Whilst not a legal requirement, in accordance with Council Procedure Rule 10 and in the interests of clarity and transparency, Members should declare any disclosable pecuniary interests which they have already declared in the Register at this point in the meeting.

In accordance with Part B, Section 2, of the Code of Conduct, Members are required to declare the existence and nature of any other interests as defined in paragraphs 8(1) or 9(2) of the Code of Conduct.

5. **Annual Audit Letter - 2013/14** (Pages 1 - 7)

Report of KPMG

6. **Fraud Briefing 2014** (Pages 8 - 20)

Report of the Audit Commission

7. **Internal Audit Monitoring Report** (Pages 21 - 27)

Report of Internal Audit Manager

8. **Development of Internal Audit and Assurance** (Pages 28 - 39)

Report of Internal Audit Manager

9. **Regulation of Investigatory Powers (RIPA)** (Pages 40 - 66)

Report of Internal Audit Manager

ADMINISTRATIVE ARRANGEMENTS

(i) Membership

Councillors Malcolm Thomas (Chairman), Geoff Knight (Vice-Chairman), Jon Barry, Richard Newman-Thompson, Elizabeth Scott, David Whitaker and Peter Williamson

(ii) Substitute Membership

Councillors Roger Dennison, Tim Hamilton-Cox, Geoff Marsland, Sylvia Rogerson, Roger Sherlock and Susan Sykes

(iii) Queries regarding this Agenda

Please contact Jane Glenton, Democratic Services - telephone (01524) 582068, or email jglenton@lancaster.gov.uk.

(iv) Changes to Membership, substitutions or apologies

Please contact Members' Secretary, telephone (01524) 582170, or email memberservices@lancaster.gov.uk.

MARK CULLINAN,
CHIEF EXECUTIVE,
TOWN HALL,
DALTON SQUARE,
LANCASTER, LA1 1PJ

Published on Tuesday, 13 January 2015.



cutting through complexity™

Annual Audit Letter 2013/14

Lancaster City Council

October 2014



The contacts at KPMG in connection with this report are:

Timothy Cutler
Partner
KPMG LLP (UK)

Tel: 0161 246 4774
tim.cutler@kpmg.co.uk

Richard Lee
Senior Manager
KPMG LLP (UK)

Tel: 0161 246 4661
richard.lee@kpmg.co.uk

Sukhsimran Singh
Assistant Manager
KPMG LLP (UK)

Tel: 0161 246 4668
sukhsimran.singh@kpmg.co.uk

Page

Report sections

- Headlines

Appendices

1. Summary of reports issued
2. Audit fees

2

4

5

This report is addressed to the Authority and has been prepared for the sole use of the Authority. We take no responsibility to any member of staff acting in their individual capacities, or to third parties. The Audit Commission has issued a document entitled *Statement of Responsibilities of Auditors and Audited Bodies*. This summarises where the responsibilities of auditors begin and end and what is expected from the audited body. We draw your attention to this document which is available on the Audit Commission's website at www.auditcommission.gov.uk.

External auditors do not act as a substitute for the audited body's own responsibility for putting in place proper arrangements to ensure that public business is conducted in accordance with the law and proper standards, and that public money is safeguarded and properly accounted for, and used economically, efficiently and effectively.

If you have any concerns or are dissatisfied with any part of KPMG's work, in the first instance you should contact Timothy Cutler, the appointed engagement lead to the Authority, who will try to resolve your complaint. If you are dissatisfied with your response please contact Trevor Rees on 0161 246 4000, or by email to trevor.rees@kpmg.co.uk, who is the national contact partner for all of KPMG's work with the Audit Commission. After this, if you are still dissatisfied with how your complaint has been handled you can access the Audit Commission's complaints procedure. Put your complaint in writing to the Complaints Unit Manager, Audit Commission, 3rd Floor, Fry Building, 2 Marsham Street, London, SW1P 4DF or by email to complaints@audit-commission.gsi.gov.uk. Their telephone number is 0303 4448 330.

Section one
Headlines



This report summarises the key findings from our 2013/14 audit of Lancaster City Council (the Authority).

Although this letter is addressed to the Members of the Authority, it is also intended to communicate these issues to key external stakeholders, including members of the public.

Our audit covers the audit of the Authority's 2013/14 financial statements and the 2013/14 VFM conclusion.

<p>VFM conclusion</p>	<p>We issued an unqualified conclusion on the Authority's arrangements to secure value for money (VFM conclusion) for 2013/14 on 17 September 2014. This means we are satisfied that you have proper arrangements for securing financial resilience and challenging how you secure economy, efficiency and effectiveness.</p> <p>To arrive at our conclusion we looked at your financial governance, financial planning and financial control processes, as well as how you are prioritising resources and improving efficiency and productivity.</p>
<p>VFM risk areas</p>	<p>We identified a number of significant risks to our VFM conclusion and considered the arrangements you have put in place to mitigate these.</p> <p>Our work identified the following:</p> <ul style="list-style-type: none"> ■ The organisation has robust systems and processes to manage effectively financial risks and opportunities, and to secure a stable financial position that enables it to continue to operate for the foreseeable future. ■ The organisation is prioritising its resources within tighter budgets, for example by achieving cost reductions and by improving efficiency and productivity. <p>We have concluded that the Authority has made proper arrangements to secure economy, efficiency and effectiveness in its use of resources.</p>
<p>Audit opinion</p>	<p>We issued an unqualified opinion on your financial statements on 17 September 2014. This means that we believe the financial statements give a true and fair view of the financial position of the Authority and of its expenditure and income for the year.</p>
<p>Financial statements audit</p>	<p>We identified one significant audit risk during the audit and reported this to the Audit Committee in our Audit Highlights Memorandum. A summary of this risk and our findings is detailed below:</p> <ul style="list-style-type: none"> ■ As a result of the introduction of the Business Rates Retention Scheme, the Authority was required to recognise a provision within the financial statements which estimates the potential cost of outstanding business rate appeals up until 31 March 2014. As the calculation of the provision required management to make significant assumptions and judgements in relation to Lancaster's hereditaments under appeal, in particular, the two power stations, management chose to use an expert, Inform-CPI, to assist them in calculating the provision. Following our audit work, we were satisfied with the basis of the estimate for the NNDR provision included within the financial statements.
<p>Annual Governance Statement</p>	<p>We reviewed your <i>Annual Governance Statement</i> and concluded that it was consistent with our understanding.</p>

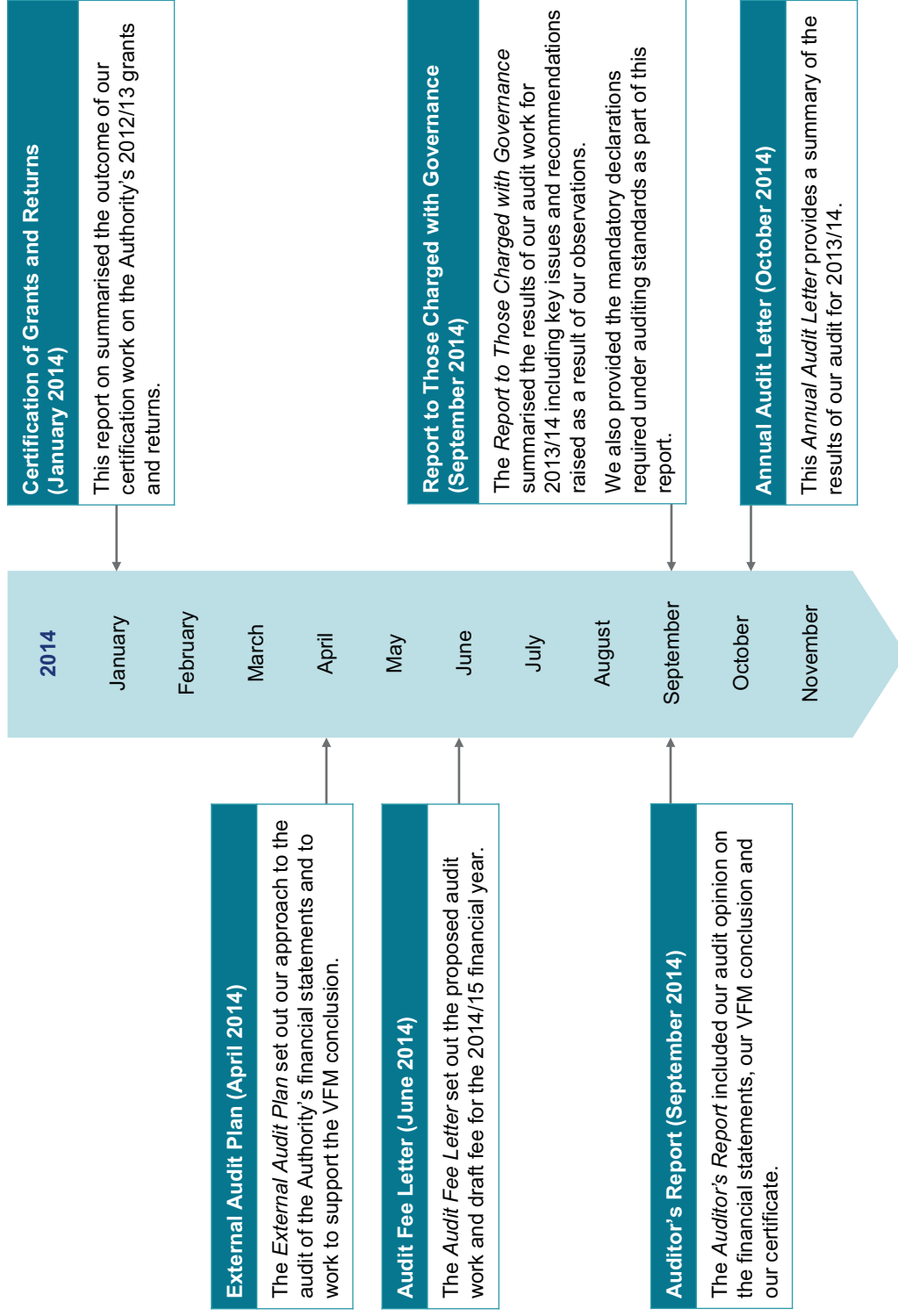
We provide a summary of our key recommendations in Appendix 1.

All the issues in this letter have been previously reported. The detailed findings are contained in the reports we have listed in Appendix 2.

Whole of Government Accounts	We reviewed the consolidation pack which the Authority prepared to support the production of Whole of Government Accounts by HM Treasury. We reported that the Authority's pack was consistent with the audited financial statements.
High priority recommendations	No high priority recommendations were identified as a result of our 2013/14 audit work. Lower priority recommendations have been reported, as appropriate, in our Audit Highlights Memorandum.
Certificate	We issued our certificate on 17 September 2014. The certificate confirms that we have concluded the audit for 2013/14 in accordance with the requirements of the <i>Audit Commission Act 1998</i> and the Audit Commission's <i>Code of Audit Practice</i> .
Audit fee	Our proposed final fee for 2013/14 is £82,881, excluding VAT. This represents a £5,931 increase on the planned audit fee (£76,950) due to the additional work required as part of the audit. Audit Commission fee variations have been raised for the additional work; further detail is contained in Appendix 2.

Appendix 1: Summary of reports issued

This appendix summarises the reports we issued since our last *Annual Audit Letter*.



This appendix provides information on our final fees for 2013/14.

To ensure openness between KPMG and your Audit Committee about the extent of our fee relationship with you, we have summarised the outturn against the 2013/14 planned audit fee.

External audit

Our proposed final fee for 2013/14 audit of the Authority is £82,881, excluding VAT. This represents a £5,931 increase on the planned audit fee of £76,950. Three Audit Commission fee variations have been raised for the additional fee, one of which has been approved and the other two are currently being reviewed. The fee variations are a result of:

- additional work in relation to a request for a public interest investigation and report. £3,462 fee variation approved;
- the additional risk-based work required to obtain assurance over the NDR appeals provision included in the 2013/14 financial statements. £1,569 fee variation under review; and
- the additional work we have undertaken on the financial statements audit, as a result of not certifying LA01 (the NNDR3 return). £900 fee variation under review.

We will only invoice the outstanding fee variations once the Audit Commission has approved them.

Certification of grants and returns

Our grants work is still ongoing and the fee will be confirmed through our report on the *Certification of Grants and Returns 2013/14* which we are due to issue in January 2015.



cutting through complexity™

© 2014 KPMG LLP, a UK public limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative, a Swiss entity. All rights reserved.

The KPMG name, logo and 'cutting through complexity' are registered trademarks or trademarks of KPMG International Cooperative (KPMG International).

Protecting the Public Purse Fraud Briefing 2014 Lancaster City Council



Purpose of Fraud Briefing



Provide an information source to support councillors in considering their council's fraud detection activities



Extend an opportunity for councillors to consider fraud detection performance, compared to similar local authorities



Give focus to discussing local and national fraud risks, reflect on local priorities and the proportionate responses needed



Be a catalyst for reviewing the council's current strategy, resources and capability for tackling fraud

Understanding the bar charts

Outcomes for the first measure for your council are highlighted in yellow in the bar charts. The results of your comparator authorities are shown in the green bars.



Outcomes for the second measure for your council are highlighted as a green symbol above each bar. The results of your comparator authorities are shown in the white triangles.



A ‘*’ symbol has been used on the horizontal axis to indicate your council.

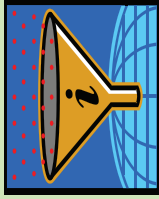
All data are drawn from council submissions on the Audit Commission's annual fraud and corruption survey for the financial year 2013/14.

In some cases, council report they have detected fraud and do not report the number of cases and/or the value. For the purposes of this fraud briefing these 'Not Recorded' records are shown as Nil.

Comparator group

Broxtowe	Preston
Burnley	Ribble Valley
Canterbury	Rossendale
Chorley	Scarborough
Dover	Sedgemoor
Eastleigh	Shepway
Fylde	South Ribble
Gedling	Swale
Havant	West Lancashire
Hyndburn	Weymouth and Portland
Lancaster	Wyre
Newcastle Under Lyme	Wyre Forrest
North Devon	
Pendle	

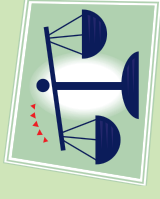
Interpreting fraud detection results



Contextual and comparative information needed to interpret results



Detected fraud is indicative, not definitive, of counter fraud performance (*Prevention and deterrence should not be overlooked*)



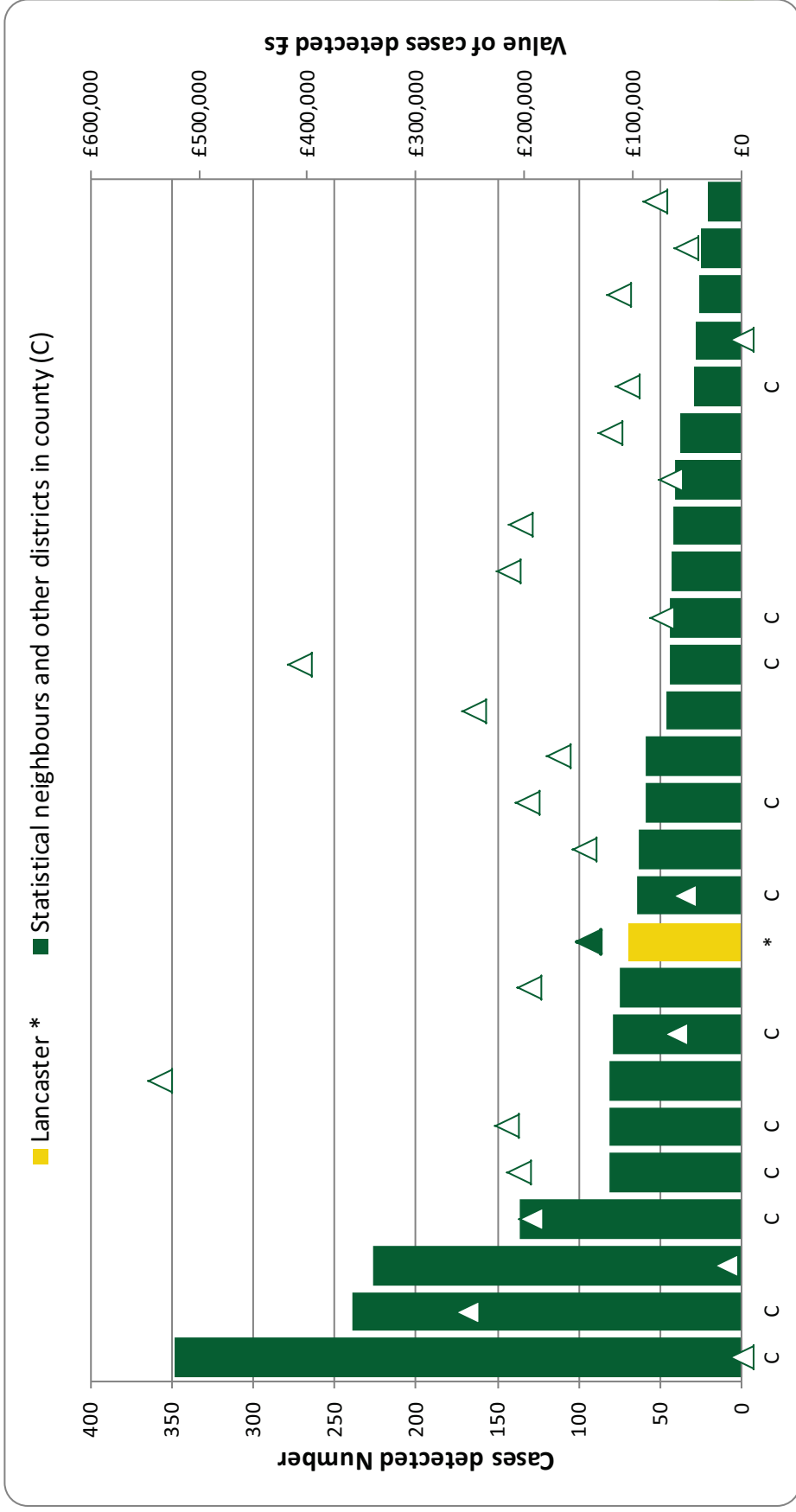
No fraud detected does not mean no fraud committed (*Fraud will always be attempted and even with the best prevention measures some will succeed*)



Councils who look for fraud, and look in the right way, will find fraud (*There is no such thing as a small fraud, just a fraud that has been detected early*)

Total detected cases and value 2013/14 (Excludes Housing tenancy fraud)

Lancaster



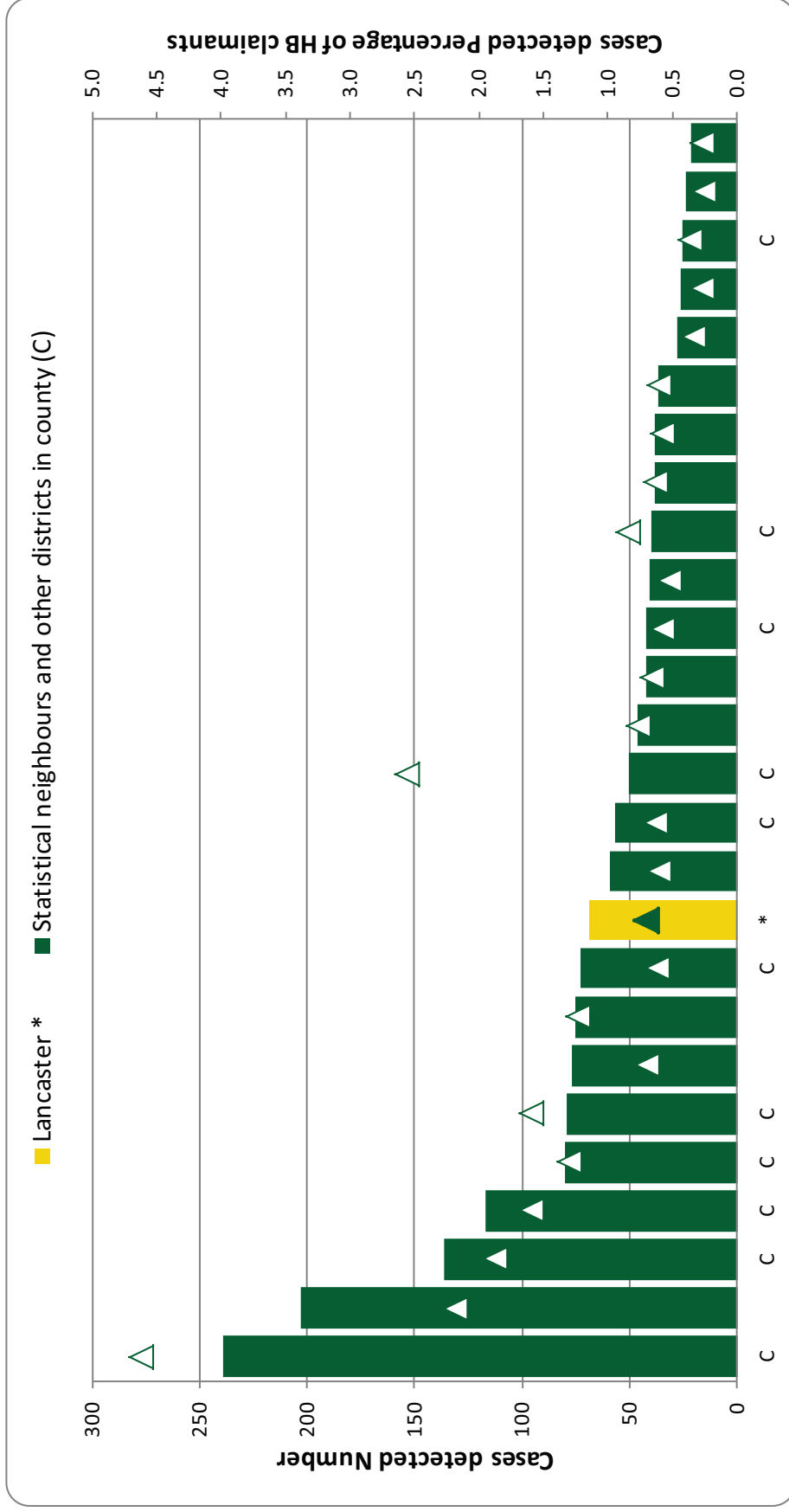
Lancaster detected 69 cases. The value of detected fraud was £139,667.
 Average for statistical neighbours and county: 81 cases, valued at £156,689.



Housing Benefit (HB) and Council Tax Benefit (CTB) 2013/14

Total detected cases, and as a proportion of housing benefit caseload

Lancaster



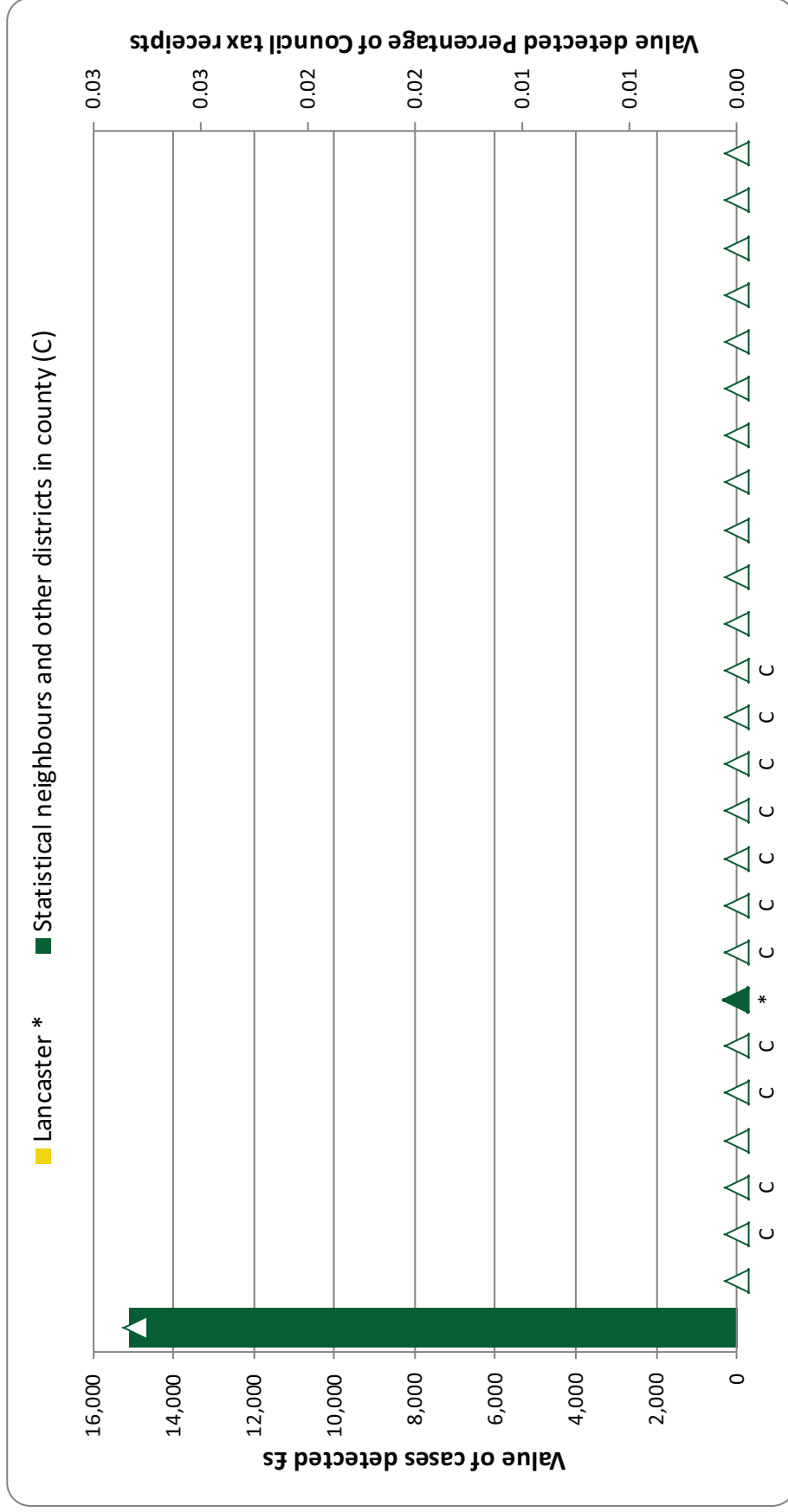
Lancaster detected 69 cases of this type of fraud. The value of detected fraud was £139,667.
 Average for statistical neighbours and county: 68 cases, valued at £176,233



Council tax discount fraud 2013/14

Total detected cases, and as a proportion of council tax income

Lancaster



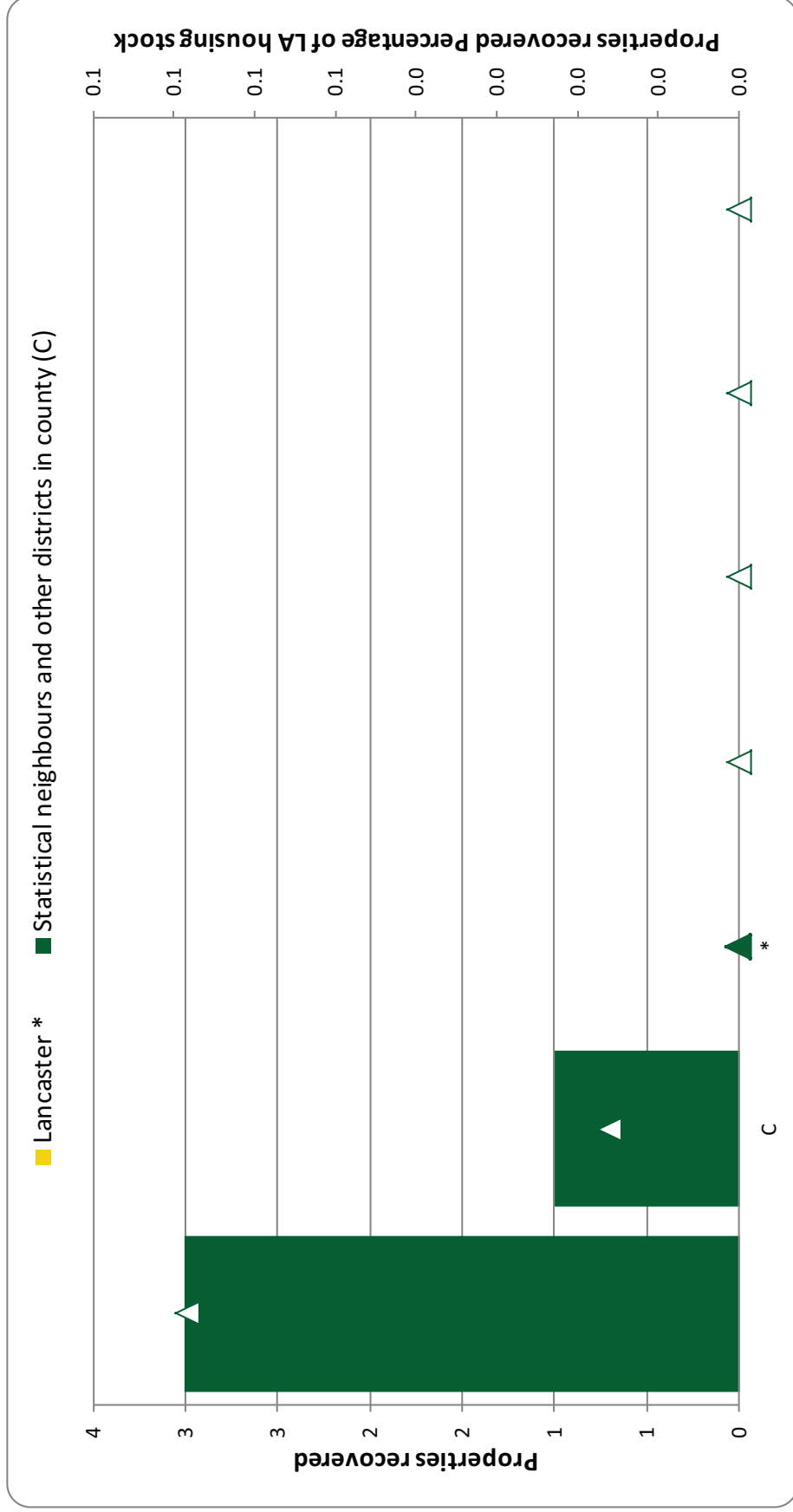
Lancaster detected 0 cases.
 Average for statistical neighbours and county: 8 cases, valued at £604.



Social Housing fraud (only councils with housing stock) 2013/14

Total properties recovered, and as a proportion of housing stock

Lancaster



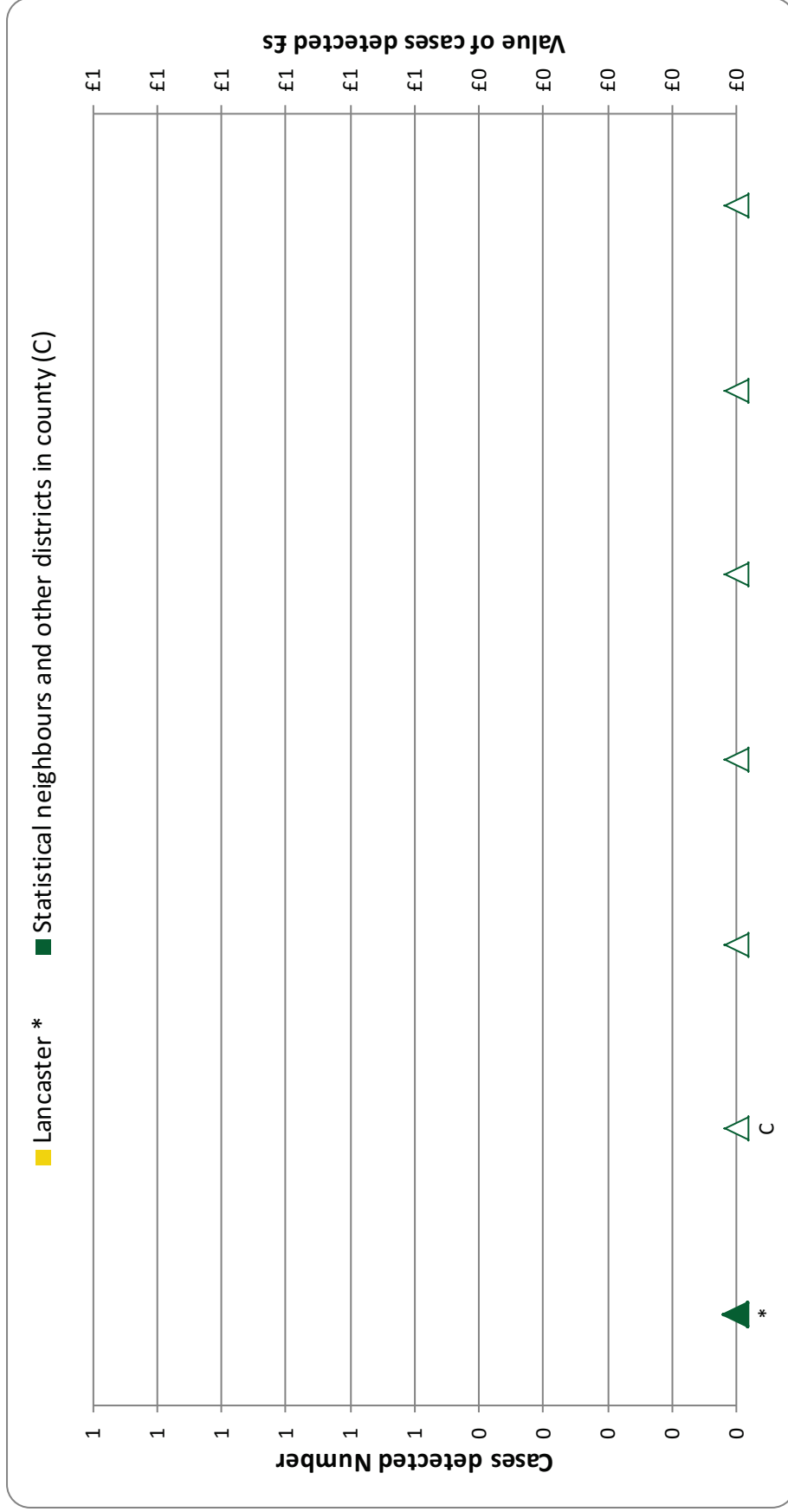
Lancaster did not detect any cases of this type of fraud.
 Average for statistical neighbours and county with housing stock: 1 case



Right to buy fraud (only councils with housing stock) 2013/14

Right to buy cases and value

Lancaster



Lancaster did not detect any cases of this type of fraud.
 Average for statistical neighbours and county with stock: 0 cases.



Other frauds 2013/14

Lancaster

Procurement: Lancaster did not detect any cases of this type of fraud.
Total for statistical neighbours and county: 1 case, valued at £0

Insurance: Lancaster did not detect any cases of this type of fraud.
Total for statistical neighbours and county: 1 case, valued at £4,500

Economic and third sector: Lancaster did not detect any cases of this type of fraud.
Total for statistical neighbours and county: 0 cases

Internal: Lancaster detected this type of fraud and did not report the number of cases.
Total for statistical neighbours and county: 10 cases, valued at £27,648

Correctly recording fraud levels is a central element in assessing fraud risk.

It is best practice to record the financial value of each detected case

Questions elected members and decision makers may wish to ask

Post SFIS

Are our remaining counter-fraud resources and skill sets adequate after our benefit fraud investigators have left to join SFIS?

Local priorities

Are local priorities reflected in our approach to countering fraud?

Partnerships

Have we considered counter-fraud partnership working?

Using information and data

Are we satisfied that we will have access to comparative information and data to inform our counter-fraud decision making in the future?

Any questions?



AUDIT COMMITTEE**Internal Audit Monitoring Report
21st January 2015****Report of Internal Audit Manager****PURPOSE OF REPORT**

To advise Members of the latest monitoring position regarding the 2014/15 Internal Audit Plan, seek approval for proposed variations to the plan, and update Members on the results of recent audits.

This report is public

RECOMMENDATIONS

- (1) That the current monitoring position is noted.
- (2) That the proposed revisions to the audit plan, as set out in the table in §1.2, are approved.
- (3) That the results of recent audits (sections 2-3 of the report) are noted.

1.0 Audit Plan Monitoring to 30th December 2014

- 1.1 Audit Committee approved the 2014/15 Internal Audit Plan at its meeting on 18th June 2014 and approved a number of adjustments at its meeting on 17th September 2014. This report is based on the monitoring position up to 30th December 2014 and a detailed monitoring report as at that date is attached as Appendix A. In summary, the position at that date was as shown in the following table.

1.2 Summary of monitoring position at 30th December 2014

Area of work	Resources (audit days)					
	Actuals to 30/12/14	Remain-ing	Comm-itted	Current Plan	Variance	Proposed Plan
Assurance Work						
Core Financial Systems	21	5	26	50	24	40
Revenues & Benefits Shared Services	46	14	60	60	0	60
Core Management Arrangements	31	9	40	50	10	40
Risk Based Assurance Audits	105	0	105	155	50	125
Follow-Up Reviews	53	10	63	50	(13)	63
Sub-Total, Assurance	256	43	299	365	66	328
Consultancy Work						
Support Work	36	8	44	35	(9)	44
Corporate service review work	19	0	19	50	31	19
Ad-Hoc Advice	56	9	65	80	15	65
Sub-Total, Consultancy	111	17	128	165	37	128
Other Work						
Other Duties (Non-Audit)	14	5	19	10	(9)	19
Work for Other Bodies	28	27	55	50	(5)	55
Audit Management	35	15	50	50	0	50
Sub-Total, Other Work	77	47	124	110	(14)	124
Contingencies						
Investigations	7	0	7	30	23	7
General Contingency	0	0	0	20	20	0
Sub-Total, Contingencies	7	0	7	50	43	7
Total	451	107	558	690	132	587

1.3 The monitoring position takes account of ongoing and planned work commitments. This shows that overall, current commitments total 558 days compared with the current plan of 690 days, giving an uncommitted resource of 119 days. This includes both the balance of the general contingency of 20 days and the unallocated balance of the contingency for investigation work (23 days).

1.4 The Internal Audit section currently has a vacancy in the Principal Auditor post. Proposals relating to developing the Council's information governance, anti-fraud and corporate assurance arrangements, all of which are linked with the Internal Audit service are dealt with in a separate report on this agenda.

Proposals

1.5 The loss of resources from the post vacancy has been partly mitigated by temporarily increasing the Assistant Auditor's working hours. Taking account of these factors, Internal Audit resources available for the remainder of the year amount to 136 days, giving a total for the year of 587. This represents an overall reduction of 103 against the current plan.

1.6 When resource availability is an issue, priority is given to maintaining the programme of Assurance Work. It is therefore proposed that the shortfall is initially met by:

- a reduction of 31 days in work supporting the corporate service review programme. There are no current or planned calls on internal audit time to support this programme;
- reduced levels of ad-hoc advice, freeing up 15 days;
- applying the remaining 20 days of the General Contingency and the remaining 23 days in the contingency to cover investigations.

1.7 Taking account of these adjustments and other variances in the plan, there remains a shortfall of 37 days in the Assurance Work programme. Taken alongside the earlier reduction of 15 days, approved by the Committee in September 2014, this represents a sizeable change (approximately 14%) in the original plan. Options available within existing staffing budgets, including the engagement of temporary staff, are therefore being considered to manage and reduce this impact.

Work for Other Bodies

1.8 As previously reported to the Committee, Internal Audit have been providing services to the Lake District National Park Authority (LDNPA) for the past two years. The LDNPA has recently completed a tendering exercise and appointed an alternative supplier for its future internal audit service. Given the review being undertaken of internal audit and assurance and related functions within the Council and the uncertainties that these presented, a decision was taken not to tender for the contract on this occasion.

2.0 Results of Internal Audit Work to 30th December 2014

2.1 This report covers audit work and reports issued since the last update report to Committee on 17th September 2014. Summary reports have been issued to Members for consideration and are also posted on the Council's Intranet. The reports issued have been:

Audit Title		Report Date	Assurance Level	
New Audit Reports				
14/0937	Council Tax	27/11/14	Substantial	✓
14/0938	Non-Domestic Rates	03/12/14	Substantial	✓

Follow up Reviews				
13/0871	HR System Replacement	16/12/14	Substantial	✓
13/0877	Corporate Property Related Service Contracts	03/12/14	Limited	⚠
13/0895	Trade Waste and Recycling, Bulky Waste and Litter Enforcement Fees and Charges	19/11/14	Substantial	✓
13/0897	CCTV	16/12/14	Limited	⚠
13/0906	Revenues & Benefits Operational Support	03/12/14	Substantial	✓
14/0916	Fleet Management	12/01/15	Substantial	✓
14/0922	Salt Ayre Sports Centre – Financial Procedures	24/12/14	Limited	⚠

3.0 Matters Arising from Audit Reviews

3.1 The key conclusions and action points in relation to those reports where a “Limited” or “Minimal” assurance opinion has been given are:

3.2 13/0877 - Corporate Property Related Service Contracts (Limited)

Good progress has been made with implementation of the action plan resulting from the original review, with all actions agreed being in the process of being implemented. Work is ongoing to centralise the management of property related service contracts with a view to a more coordinated, corporate approach being achieved. A more structured and automated approach to monitoring compliance is also being developed. Once these arrangements have been fully implemented a substantial level of assurance should be achieved.

3.3 13/0897 - CCTV (Limited)

Due to staffing changes in relation to CCTV management, implementation of the agreed action plan has been delayed. However, good progress is now being made to address the issues identified in the original audit. Responsible officers have made significant headway in bringing themselves up to speed with the requirements of the Code of Practice and related legislation. The CCTV Officer Working Group is also keen to make the improvements required to ensure that the council is fully compliant as necessary. Once the agreed action plan has been fully implemented a substantial level of assurance should be achieved.

3.4 14/0922 - Salt Ayre - Financial Procedures (Limited)

Good progress has been made to streamline arrangements at SASC and procedures and processes have been made more efficient and effective in many of the areas identified during the original review. However, stock management arrangements and the streamlining of processes relating to the input and authorisation of overtime claims are still in the process of being addressed and until this work is complete the assurance opinion will remain at limited.

3.5 Given the current position on each of these three reviews, it is proposed that Internal Audit continues to track progress over the coming year and report developments to future meetings of the Audit Committee.

4.0 Details of Consultation

4.1 Management Team continues to be consulted in developing the plan.

5.0 Options and Options Analysis (including risk assessment)

5.1 Regarding the Internal Audit Plan, the options available to the Committee are either to approve the proposed changes, which seek to maintain as far as possible the level of resources devoted to the provision of assurance, or to propose an alternative course of action.

6.0 Conclusion

6.1 A significant realignment of remaining plan allocations is required to manage the availability and use of internal audit resources over the final quarter of the financial year. Pending the approval and implementation of proposals concerning the future structure and remit of internal audit, arrangements are being made to manage the plan and associated resources so as to maintain the level of independent assurance provided to the Committee and the Council.

CONCLUSION OF IMPACT ASSESSMENT

(including Diversity, Human Rights, Community Safety, Sustainability and Rural Proofing)

Not applicable

FINANCIAL IMPLICATIONS

None directly arising from this report

SECTION 151 OFFICER'S COMMENTS

The Section 151 Officer has been consulted and has no further comments

LEGAL IMPLICATIONS

None directly arising from this report

MONITORING OFFICER'S COMMENTS

The Monitoring Officer has been consulted and has no further comments

BACKGROUND PAPERS

























Internal Audit Plan 2014/15

Contact Officer: Derek Whiteway

Telephone: 01524 582028

E-mail: dwhiteway@lancaster.gov.uk

Ref: aud/comm/audit/150121IAMon

Work Allocations		Actuals to 30/12/14	Remaining	Committed	Approved Plan (17/09/14)	Variance	Status at 30/12/14
Job No	Title						
1. ASSURANCE WORK							
LCC Core Financial Systems							
14/0925	Payroll	13	5	18			
14/0927	General Ledger Coding	8	0	8			
Sub-total - Core Financial Systems		21	5	26	50	24	
Revenues Shared Service - Financial Systems							
14/0929	Housing Benefits 2014/15 - Preston CC	5	6	11			
14/0930	Council Tax 2014/15 - Preston CC	6	0	6			
14/0931	NNDR 2014/15 - Preston CC	13	0	13			
14/0932	Operations and Performance 2014/15 - Preston CC	3	2	5			
14/0936	Housing Benefits 2014/15 - Lancaster CC	4	5	9			
14/0937	Council Tax 2014/15 - Lancaster CC	4	0	4			
14/0938	NNDR 2014/15 - Lancaster CC	9	0	9			
14/0939	Operations and Performance 2014/15 - Lancaster CC	2	1	3			
Sub-total - Revenues Shared Services		46	14	60	60	0	
Core Management Arrangements							
13/0871	HR Systems Replacement	1	0	1			
13/0903	National Fraud Initiative 2012/13	7	0	7			
14/0917	National Fraud Initiative 2014/15	13	9	22			
14/0919	Internal Communications	2	0	2			
14/0923	Annual Governance Review and Statement 2013/14	8	0	8			
Sub-total - Core Management Arrangements		31	9	40	50	10	
Risk Based Assurance Work Programme							
13/0908	Commercial Property Leases and Licences	1	0	1			
13/0911	Officer Gifts, Hospitality and Register of Interests	3	0	3			
14/0916	Fleet Management	6	0	6			
14/0918	Planning - Strategic Housing Market Assessment	29	0	29			
14/0920	Council Housing Tenancy Fraud	17	0	17			
14/0921	Outdoor Events Management	19	0	19			
14/0922	Salt Ayre Sports Centre - Financial Procedures	10	0	10			
14/0924	Housing Options and Allocations	20	0	20			
Sub-total - Risk Based Assurance Work		105	0	105	155	50	
Follow-Up Reviews		53	15	68	50	-18	
SUB-TOTAL - ASSURANCE WORK		256	43	299	365	66	

Work Allocations		Actuals to 30/12/14	Remaining	Committed	Approved Plan (17/09/14)	Variance	Status at 30/12/14
Job No	Title						
2. CONSULTANCY WORK							
Support Work (projects and other)							
12/0849	Complaints - Officer Working Group	4	0	4			✓
13/0876	Financial Regulations Review	20	5	25			⚠
14/0928	Procurement Strategy Development	6	0	6			✓
14/0509	RIPA Monitoring and Central Register	1	1	2			⚠
14/0941	Fuel Cards	5	2	7			⚠
Sub-total - Support Work (projects and other)		36	8	44	35	-9	
Corporate Service Reviews							
13/0910	Ordering and Payment Systems Review	5	0	5			✓
14/0934	Business Travel and Transport Review	14	0	14			✓
Sub-total - Corporate Service Reviews		19	0	19	50	31	
Ad-Hoc Advice		56	9	65	80	15	∞
SUB-TOTAL - CONSULTANCY WORK		111	17	128	165	37	
3. OTHER							
12/0392	Deputy s151 Officer Duties	14	5	19	10	-9	∞
	Audit Work for Other Bodies - LDNPA	28	27	55	50	-5	⚠
SUB-TOTAL - OTHER		42	32	74	60	-14	
4. AUDIT MANAGEMENT							
12/0172	Committee Work	12	5	17			∞
12/0189	Audit Planning & Monitoring	23	10	33			∞
SUB-TOTAL - AUDIT MANAGEMENT		35	15	50	50	0	
5. CONTINGENCIES							
Investigations		7	0	7	30	23	
General Contingency		0	0	0	20	20	
SUB-TOTAL - CONTINGENCIES		7	0	7	50	43	
TOTALS		451	107	558	690	132	

Key: ✓ Completed ⚠ In Progress ? Not Yet Started ∞ Continuous or Multi-Year Activity
 CFwd Carried Forward to 2015/16 Plan ✗ Abandoned

AUDIT COMMITTEE

**Development of Internal Audit and Assurance
21st January 2015**

Report of Internal Audit Manager

PURPOSE OF REPORT

To seek the Committee’s support for proposals for strengthening the Council’s information governance and other assurance arrangements (covering Information and Communications Technology (ICT), information management, corporate anti-fraud and internal audit generally)

This report is public

RECOMMENDATIONS

- (1) That the Audit Committee supports proposals for the development of the ICT service and the corporate information governance function as outlined in the report.**
- (2) That Audit Committee supports the setting-up of a corporate anti-fraud team in collaboration with Preston City Council and Fylde Borough Council on the basis outlined in the report.**
- (3) That Audit Committee supports proposals for the development of assurance reporting and endorses the proposed widening of the Internal Audit service’s remit.**

1 Introduction

1.1 The Audit Committee’s terms of reference include:

8.2 To monitor arrangements for discharging the Council’s responsibilities for efficient and effective financial and operational resource management...; and

8.18 To monitor the effective development and operation of risk management and corporate governance...

1.2 As part of the 2014/15 budget, Cabinet supported an outline investment plan and associated growth estimated at £120K per year for ICT security and Public Services Network (PSN) compliance. The growth was duly approved at Budget Council on 26 February 2014, its future use being subject to a further report to Cabinet.

1.3 Linked to this, the Council’s positioning regarding information governance has been commented on in the last two Annual Governance Statements. The 2013/14 statement, approved by Audit Committee in September 2014, acknowledged that, following a significant body of work surrounding the Public Services Network (PSN), further actions were still required *“to ensure that the council’s arrangements for collecting, storing, using and sharing information are robust and enable the most efficient and effective use of that information”*.

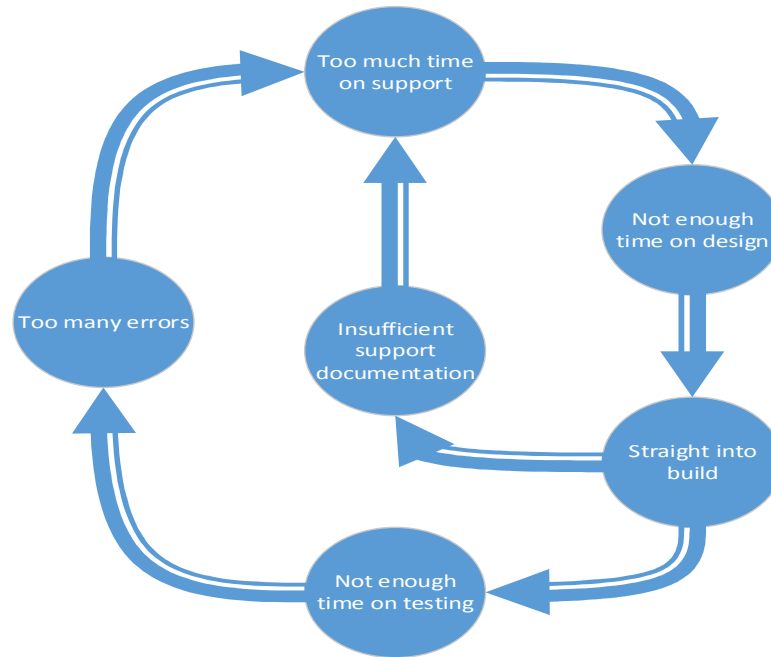
1.4 In addition to addressing those needs from both ICT and general information governance perspectives, this report takes the opportunity to consider the Council’s response to other recent developments regarding anti-fraud arrangements.

2 Information Security and Governance

2.1 Information and Communications Technology (ICT)

- 2.2 Sound ICT is essential for effective service delivery and as such, any delays, outages or other difficulties in the supply of the ICT service can have significant adverse impact, potentially across the whole organisation. This is recognised, hence the approval of the budget growth almost a year ago.
- 2.3 In terms of the PSN, after a very difficult exercise under a very stringent regime, compliance was first gained in May 2014. Nationally, the arrangements have been the subject of criticism, because of inconsistencies in assessment experiences of various councils to some degree but more fundamentally, because of an imbalance in the absolute need for addressing real and perceived security risks at the expense of service provision – with the latter losing out significantly in some cases. Moreover, indications are that it has proved a very expensive exercise for local government as a whole.
- 2.4 That is not to say that there have been no benefits derived from the experience, however. On a more positive note, the Council does have a far more robust ICT network and Officers have already learned much, in getting this far. It is also apparent that Government has recognised councils' difficulties and it is committed to improving arrangements.
- 2.5 Unfortunately though, this was not in time to influence the timing of the Council's subsequent PSN assessment, as this still had to be completed and submitted last August, only 3 months after gaining the last accreditation. Once again this tied up resources and resulted in additional costs, although by no means to the extent experienced on the previous occasion. Nonetheless, it did result in further delays in progressing the more proactive work to develop service restructure proposals for the future. The £120K additional budget available in this year has been spent on putting in place infrastructure and interim consultancy support to resolve outstanding tasks from the first PSN assessment, as well as dealing with the requirements of the second one.
- 2.6 Government's change in stance has influenced its response to the second assessment, however. Officers have only very recently received any actual feedback; initial indications are encouraging and it is hoped that confirmation of compliance will be received sometime this month.
- 2.7 More specifically, Government has now brought in significant changes for the governance for PSN. For example, it has established a PSN Programme Board to help improve the compliance process and capitalise on the opportunities that PSN presents, such as supporting the joining up of public services in an efficient and effective manner. The Local Government Association (LGA), the public sector based Society of IT Management (SOCITM) and other local authority representatives are included on the Board. Furthermore, the Council's ICT Manager is currently the Regional Chair for SOCITM in the North West, which gives a good opportunity to both contribute to and keep abreast of future developments.
- 2.8 Whilst undertaking the network security remediation work in order to meet PSN requirements, it became very clear that ways of working and skills levels within ICT required strengthening to meet and keep up to date with industry standards. Developing appropriate plans to tackle this takes time, however – especially as day to day service provision must continue. An external company was engaged to undertake a skills review, in order to inform restructuring proposals.

2.9 As background, the current structure of three teams within ICT, (these being Service Desk, Technical Support and Applications Support), has been in place for at least the last 15 years. Staff in each section have to prioritise their work between support and development and often, as a result, areas of development including design, testing, and hand-over to Service Desk, are sacrificed. Instead, just trying to get and keep systems up and running becomes the priority. With the focus being on resolving issues that arise from this, there has been inadequate time to devote to strategy. The following diagram sums up the service’s way of working, which in the industry is referred to as a “circle of too much support”.



2.10 In short, the key findings of the external review were therefore as expected, in that the ICT service is understaffed and under-skilled in critical areas. Furthermore, the service also needs to draw on external support where this is more cost-effective to do so, for example in the provision and support for wi-fi and other aspects where 24/7 cover and support are needed.

2.11 To address this position, Cabinet has been asked to approve the development of the ICT service and restructuring proposals will be presented to Personnel Committee shortly. In the current climate of rapidly increasing change both from technology and as a result of different ways of working brought about by budget pressures, the Council needs an ICT service that provides reliable systems, manages a wide variety of technologies and is able to plan for and respond to change in an agile manner. Use of the previously approved budget growth will enable this.

2.12 **Information Governance**

2.13 In parallel with addressing ICT related vulnerabilities, it has been acknowledged that the Council also needs to develop and improve its standards of information governance generally throughout the organisation.

2.14 The key components of the Council’s current information governance arrangements are:

- Information Management Officer
- Information Management Group
- Existing policies and procedures
- On-line training resources

- 2.15 A self-assessment of the Council's current position has been carried out using the National Archive's information management self-assessment tool. A summary chart and headline results coming out of this review are set out in **Appendix A**.
- 2.16 The conclusion from this analysis is that corporately, resources and arrangements currently devoted to information management are insufficient to address the development issues identified in this review and to maintain appropriate standards into the future. Key areas for development are therefore identified as being:
- Raising understanding of the importance of 'Knowledge and Information Management' (KIM)
 - Identifying and managing significant information management risks
 - Raising understanding of the information needs of the Council and putting in place standards and procedures to ensure these are met
 - Establishing clear roles and responsibilities for information management and ensuring that staff and elected Members receive appropriate training, guidance and support
 - Developing a culture which ensures a commitment to high standards of information management and to identifying and taking advantage of information sharing opportunities
- 2.17 Given the nature of information developments, particularly those relating to digital information and the associated technology, the expectation is that resources will be required not just in the immediate term, to address the gaps identified and raise standards to an acceptable level, but also to maintain those standards into the future. Furthermore, drawing on the arrangements that other local authorities have in place, buying in support, either through collaboration with other authorities or from the private sectors, is not considered to be a viable, cost effective option, at least for the medium to longer term.
- 2.18 Accordingly, Cabinet has also been asked to approve the expansion and development of the in-house corporate information governance function, with an increase of one post being envisaged. It is proposed that managerial responsibility for Information Governance would transfer to Internal Audit.

3 Corporate Anti-Fraud Arrangements

3.1 Background

3.2 The National Fraud Authority ("NFA") estimates that fraud in local government amounts to at least £2.2 billion. In its publication "Protecting the Public Purse 2013", other than Housing/Council Tax Benefit, the Audit Commission identified a number of areas of fraud as being those that local authorities are typically likely to be subject to.

3.3 The Audit Commission goes on to say:-

"Councils face reduced funding and new national counter-fraud arrangements. They need to assess fraud risks effectively to target resources where they will produce most benefit. They should:

- *Maintain their capacity to investigate non-benefit fraud following the introduction of the Single Fraud Investigation Service ("SFIS");*
- *Follow the lead of London Boroughs and focus more effort on detecting non-benefit fraud, which directly affects their revenue; and*
- *Ensure they have the right skills to investigate all types of fraud, which vary in complexity."*

- 3.4 The public is entitled to expect the City Council to conduct its business with integrity, honesty and transparency and demand the highest standards of conduct from those working for it. Local authorities have a duty to safeguard public funds and take responsible steps to ensure this. If fraud is suspected, authorities are tasked with actively investigating allegations.
- 3.5 Historically both Lancaster and Preston City Councils have, with great success, concentrated their counter fraud work around the prevention and detection of housing benefit /council tax benefit related fraud, with occasional cases relating to other fraudulent activity or irregularity being referred to the team for further investigation.
- 3.6 The DWP contributes financially (through Housing Benefit Administration Grant) to facilitate the fraud prevention and detection work directly linked with benefit fraud.
- 3.7 Recently, however, Government has confirmed that all Local Authority Fraud Investigators will transfer to the Department of Work and Pensions (DWP) in a phased process, thus creating a Single Fraud Investigation Service (SFIS).
- 3.8 As part of these arrangements, shared service staff currently employed by Preston City Council are scheduled to transfer to DWP from 1 June 2015. This move will result in a loss of specialist resources, funding and skills. At the same time, the Council will continue to be required to participate in the National Fraud Initiative (“NFI”).
- 3.9 Additionally, the landscape in which the Council operates is changing as a result of:
- it now being responsible for determining its own Localised Council Tax Support (LCTS) Scheme;
 - Business Rates administration changes, with the potential for increased rate avoidance tactics and increased local impact; and
 - there being a higher profile regarding fraud and its impact on public funds generally, at a time when councils and other public bodies are facing huge financial challenges.
- 3.10 These factors impact directly on the scale and range of risks inherent within the Authority and its future capacity and resources. With all of these issues in mind, there is a business need to determine a suitable framework that ensures the Council is still reasonably able to prevent fraud from occurring, following the creation of SFIS. Where this is not possible, there should be a systematic and proportionate response, enabling the timely and effective detection, investigation and prosecution of fraudsters.
- 3.11 **Current Position**
- 3.12 The Council’s Financial Regulations and the Anti-Fraud, Bribery and Corruption Policy assigns responsibility for the corporate reporting and investigation of fraud and other financial irregularities to the Council’s Internal Audit function. In recent years, the majority of fraud cases detected (other than benefits) have tended to be relatively low level theft or other impropriety. There have been no cases over £10,000 requiring a report to the Audit Commission.
- 3.13 The existing shared Benefits Fraud Team consists of 10.6 full time equivalent staff operating over 3 sites. It includes counter fraud officers/managers accredited through the DWP’s Professionalism in Security (“PinS”) qualification. In addition several team members hold BTEC Professional Certificates in investigation.
- 3.14 **Proposal**
- 3.15 Cabinet has been asked to support the setting-up of a corporate anti-fraud team in collaboration with Preston City Council and Fylde Borough Council.
- 3.16 The scope of this corporate function would include business rates, council tax discounts and significantly, council tax support cases, which will not be covered by the Single Fraud Investigation Service.

- 3.17 Furthermore, under the Prevention of Social Housing Fraud Act 2013, local authorities have been given powers to investigate and prosecute tenancy fraud, providing a further opportunity to explore partnership working arrangements in social housing. This is relevant to Lancaster in relation to its own Council Housing service and in Preston, the Community Gateway Association has expressed an early interest in discussing service provision, should a shared Corporate Fraud Team be established.
- 3.18 The team would also be tasked to investigate alleged fraud, bribery and corruption by any employees, councillors, contractors, consultants, suppliers, service users and members of the public who have dealings with the Council. In summary the section will be responsible for:
- Prevention, detection, investigation and prosecution of all fraud against the Council
 - Assisting the HR Team with appropriate disciplinary matters
 - Providing assurance that the risk of fraud is minimised wherever possible
 - Working with Internal Audit on any other matters regarding fraud, bribery and corruption risks affecting the Council.
- 3.19 If this approach were to go ahead, the team would seek to work closely with other interested stakeholders, including Housing Associations and Lancashire County Council, to help detect fraud in other prime areas.
- 3.20 It is currently envisaged that a new Corporate Fraud Team established on this basis would consist of 4 posts. They would continue to be employed by Preston City Council and there would be a further partnership agreement put in place.
- 3.21 Where possible, the new Corporate Fraud Team would be staffed from the existing shared Benefit Fraud Team, ahead of the transfer to SFIS.
- 3.22 There are several options for service location and management, ranging from a virtual team located in several places, or a single unit based in one location, or a hybrid arrangement. At this stage, regardless of location, it is proposed that the Corporate Fraud Team forms part of Internal Audit resources. Officers from the partner authorities would agree the exact arrangements in due course.

3.23 Financial Implications

- 3.24 In essence, initially the proposed creation of a shared Corporate Fraud Team would be funded through redirecting the savings anticipated from the transfer of the bulk of benefit anti-fraud work to SFIS, as shown in the table below:

	2015/16	2016/17	2017/18	2018/19
Savings:	£000	£000	£000	£000
Fraud Staff TUPE – saving in LCC contribution to the Shared Service	(95)	(127)	(127)	(127)
Additional Costs				
Contribution to the Corporate Fraud Team (approx. 40%)	41	53	53	53
Administration Grant Reduction	-	74	74	74
Net Cost / (Saving)	(54)	0	0	0

- 3.25 Financial arrangements for sharing/allocating costs and savings would be developed further, drawing on the principle that the function should be self-financing, i.e. the money the team prevents being lost through fraudulent activity should more than offset the cost of running the team. The evaluation of this would be developed and monitored on an ongoing basis, to ensure that value for money is being achieved. At present, the proposal does not assume any direct savings from the team's prevention work.

- 3.26 In addition to the above, Government recently challenged Councils to use innovative financial management to tackle fraud. It set up a £16M funding pot (covering a two year period), with the purpose of encouraging bids from local authorities, working in partnership, to recoup money owed and tighten safety nets to prevent crime.
- 3.27 Preston City Council, with support from its existing local authority fraud partners (Lancaster CC & Fylde BC), submitted a successful bid for funds and it has been awarded £125,750 to help the partnership establish an investigative capacity over a 2 year period. The use of these funds has not yet been determined, but they should also mean that additional savings can be gained.
- 3.28 Separately, Officers have signed up to Government's recently announced Fraud and Error Reduction Incentive Scheme (FERIS) that runs until the end of 2015/16. This should provide financial rewards for authorities that further tackle fraud and error within their housing benefit caseload (rather than corporate fraud). The resources for participating in this will also be managed jointly, through shared arrangements.
- 3.29 As indicated earlier, the work of the proposed team will cover both General Fund and Housing Revenue Account services and each account will therefore be expected to bear an element of the Council's share of the cost. It is too early to estimate the level of cost likely to fall in each area.

4 Internal Audit and Assurance

- 4.1 Constitutionally, the Audit Committee has delegated responsibility for considering and commenting on the adequacy of Internal Audit and options for its delivery. The current structure of the Internal Audit section is as follows:

Job Type	FTE	Grade
Internal Audit Manager	1	8
Principal Auditor (vacant)	1	5
Senior Auditor	1	4
Assistant Auditor	0.8	3

- 4.2 The Internal Audit section currently has a vacancy in the post of Principal Auditor; this has been held vacant pending the proposals contained in this report and the report to Cabinet being developed and considered.

4.3 Current Position

- 4.4 Whilst the Council's Audit Committee operates substantially in accordance with recommended standards as set out by CIPFA¹, there is scope to broaden and strengthen the committee's coverage and effectiveness through developing a corporate 'assurance framework'. Currently, assurance is primarily provided to the Committee through audit reports (both Internal and External) and through its scrutiny of the production of the financial accounts.

- 4.5 The Audit Committee has a key role in considering and understanding what assurance is available to support the production of the Annual Governance Statement. Guidance therefore suggests that the Committee should be seeking to ensure that assurance is planned and delivered with the following objectives in mind:

- Clarity of what assurance is required
- Clear allocation of responsibility for providing assurance activities;
- Avoiding duplication, bearing in mind the differing objectives of assurance activities;
- Improving the efficiency and cost effectiveness of assurance

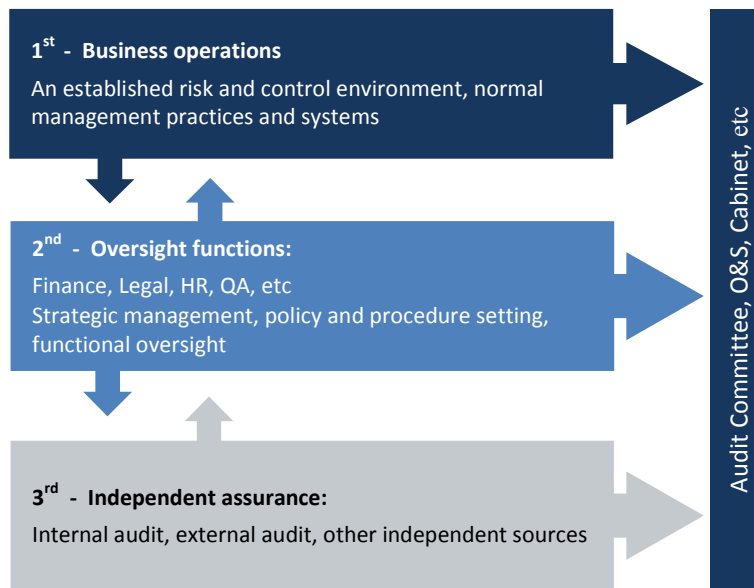
¹ Audit Committees - Practical Guidance for Local Authorities and Police (CIPFA, 2013)

- Obtaining assurance of appropriate rigour and independence across a range of assurance providers.

4.6 **Proposal**

4.7 Having a clear assurance framework in place will support the committee in considering the annual review of effectiveness for the AGS and will also support the approval of the internal audit risk-based plan, as it enables the committee to identify the extent to which it will rely on internal audit for its assurance requirements.

4.8 The ‘three lines of defence’ model (depicted in the diagram below) provides a useful way of outlining an organisation’s risk and control environment, and therefore its assurance framework.



First Line

- The first level of the control environment is the business operations which perform day-to-day risk management activity

Second Line

- Oversight functions such as Finance, Legal and HR set directions, define policy and provide assurance

Third Line

- Internal and external audit are the third line of defence, offering independent challenge to the levels of assurance provided by business operations and oversight functions.

4.9 The current vacancy within Internal Audit provides an opportunity to review the service provided and incorporate a wider ‘assurance’ function into the existing remit of Internal Audit. This would enable Internal Audit to develop and coordinate the identification and collation of assurance from across all three levels of the assurance model, with particular emphasis on the reporting of assurance to the Audit Committee.

4.10 Given the corporate nature of the work, specific responsibilities for fulfilling this wider role would be attached to the senior members of the team, i.e. the Internal Audit Manager and, to a lesser extent, the Principal Auditor.

4.11 This development would sit readily alongside enhanced roles in relation to corporate anti-fraud and information governance, should those particular proposals be taken forward. Given the Internal Audit Manager’s additional managerial commitment involved in those proposals, it is proposed that the vacant Principal Auditor post be filled and that overall, existing levels of resource in the Internal Audit team are maintained.

4.12 This approach may require some relatively minor changes to job roles within the function, but any costs involved would be minor and would be contained within existing budgets.

4.13 **Options and Options Analysis**

4.13.1 Option 1. Retain existing Internal Audit arrangements. The scope and approach of Internal Audit will remain the same;

4.13.2 Option 2. Develop a more comprehensive corporate approach to assurance through extending the remit of Internal Audit.

	Option 1- retain existing arrangements	Option 2 – incorporate responsibilities for coordinating assurance into the Internal Audit function
Advantages	None identified.	<p>An opportunity to develop corporate understanding of the Council's sources of assurance and its associated organisational performance; better value for money</p> <p>Greater clarity regarding sources of assurance; better able to avoid duplication of effort.</p> <p>Provides an opportunity for Internal Audit plans and work to be more focused on significant risk areas.</p> <p>Increased scope and effectiveness of the Audit Committee in reviewing the Council's governance arrangements</p>
Disadvantages	<p>The effectiveness of Internal Audit and the Audit Committee do not develop.</p> <p>Does not fit well with other plans for information governance and anti-fraud arrangements.</p>	None identified
Risks	Potential for wasted resources / duplication of effort through a lack of understanding about assurance	May divert resources away from other Internal Audit activity

4.14 **Officer Preferred Option**

4.15 Option 2 is preferred. As a service to the effective governance and management of the organisation, there is clear scope to develop the Council's systems for the collation and evaluation of assurance. This principle aligns well with the proposed developments in information governance and corporate anti-fraud arrangements.

5 **Details of Consultation**

5.1 Where appropriate, consultation has been undertaken with the Council's partner authorities. Any specific staffing consultation would be undertaken in accordance with the Council's protocols, where the Council is the employing authority

6 **Conclusion**

6.1 Much work has been done to develop proposals that strengthen the Council's service provision and governance arrangements, whilst containing costs within existing budgets and/or providing opportunities to secure savings. Whilst the service areas concerned may not necessarily be appreciated directly by the public, nonetheless they are essential for effective service delivery, sound governance, and the safeguarding of resources.

RELATIONSHIP TO POLICY FRAMEWORK

As stated in the Corporate Plan, a key element in ensuring its successful delivery is having sound governance arrangements in place. The proposals also fit with the Council's ethos.

CONCLUSION OF IMPACT ASSESSMENT

(including Health & Safety, Equality & Diversity, Human Rights, Community Safety, HR, Sustainability and Rural Proofing)

Any impacts would be addressed through the delivery of particular services.

LEGAL IMPLICATIONS

Legal Services have been consulted and have no observations to make in respect of the proposed anti- fraud provisions and with regards to ICT/Information Management proposals they are acceptable subject to appropriate consultation with the affected staff.

FINANCIAL IMPLICATIONS

As set out in the report.

In summary, savings of at least £84K would be achieved next year, with the potential for this to increase, predominantly through the results of anti-fraud work. Although savings should accrue from such activity in subsequent years, at present, for prudence the proposals are assumed to be budget neutral.

OTHER RESOURCE IMPLICATIONS

Human Resources/ Information Services / Property / Open Spaces:

As referred to in the report.

SECTION 151 OFFICER'S COMMENTS

The s151 Officer has been consulted and has no further comments.

MONITORING OFFICER'S COMMENTS

The Monitoring Officer has been consulted and has no comments to add.

BACKGROUND PAPERS

None.

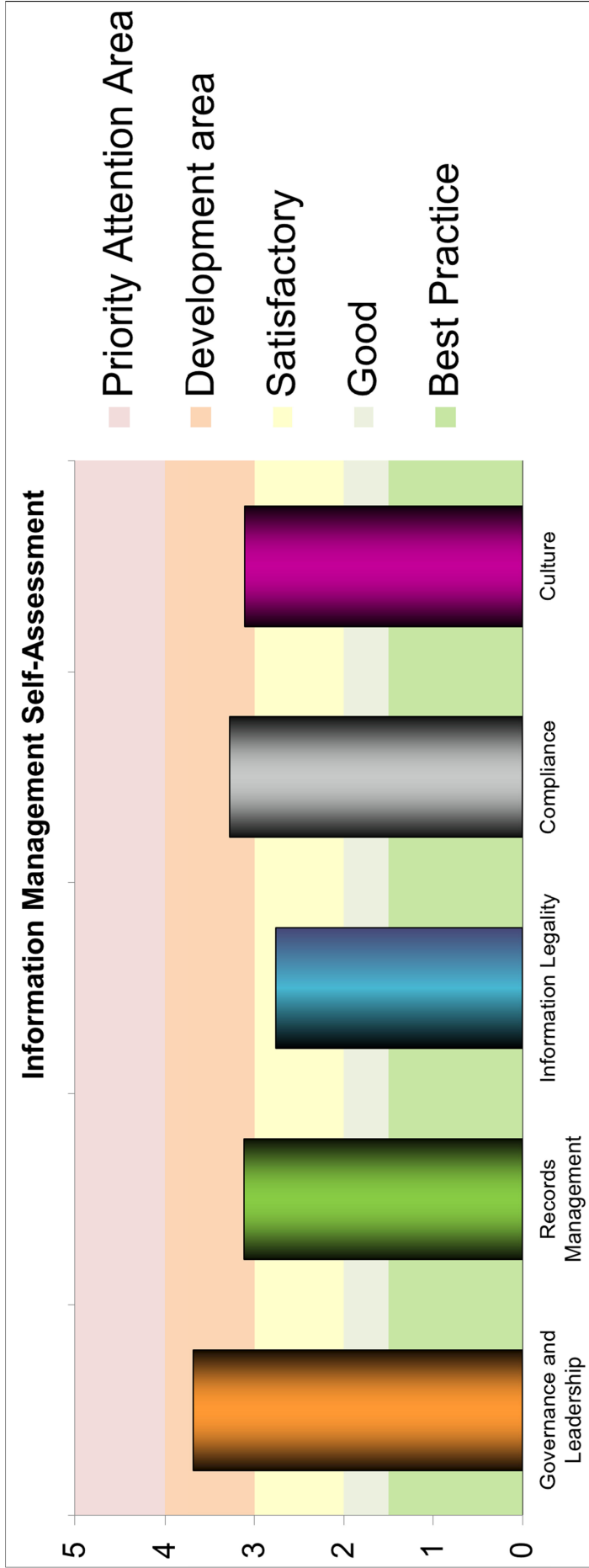
Contact Officer: Derek Whiteway

Telephone: 01524 582028

E-mail: dwhiteway@lancaster.gov.uk

Ref: aud/ctee/aud/150121/IAandAssurance

Result Chart - National Archive's Information Management Self-Assessment



Mean score per section

Framework category	Mean score per section
1 Governance and Leadership	3.68
2 Records Management	3.11
3 Information Legality	2.77
4 Compliance	3.29
5 Culture	3.11

Information Management Self-Assessment – Headline Messages

1. 4 out of the 5 categories covered in the assessment are classed as 'development areas'.
2. With the objective of meeting at least a 'Good' standard in all areas, investment is particularly required in:
 - **Governance and leadership, covering:**
 - Strategic management of 'Knowledge and Information Management' (KIM)
 - Management understanding of the importance of KIM
 - Full identification, registration and defined ownership of information assets
 - Understanding and management of the costs of KIM
 - Identification and assessment of risks to information management
 - **Records management, covering:**
 - Full understanding of the information needs of the Council and of its users
 - Establishment and implementation of clear corporate standards
 - Raising standards regarding storage, access to, and the retention and disposal of information (on both digital and physical media)
 - Developing arrangements to ensure 'digital continuity' in line with business change policies and procedures
 - Quality control and verification processes
 - **Compliance, covering:**
 - Creating clarity in roles and responsibilities for information management
 - Development of information management skills and understanding
 - Inclusion of information management considerations in change management programmes
 - Development of suitable training programmes
 - Comprehensive policies covering both digital and physical records
 - **Culture, covering:**
 - Developing management and staff commitment to high standards of information management
 - Developing understanding of KIM procedures, tools and techniques
 - Identifying and taking advantage of information sharing opportunities.

AUDIT COMMITTEE

**Regulation of Investigatory Powers (RIPA)
21st January 2015**

Report of Internal Audit Manager

PURPOSE OF REPORT

To advise Members of the Council’s current position regarding the use of surveillance and of the outcome of a recent inspection by the Office of the Surveillance Commissioner. Also to seek Members’ endorsement of the updated RIPA Policy.

This report is public

RECOMMENDATIONS

- (1) That the report is noted
- (2) That the Council’s current RIPA Policy is endorsed.

1.0 Introduction

- 1.1 Part II of the Regulation of Investigatory Powers Act 2000 (RIPA) governs public authorities’ use of covert surveillance and of “covert human intelligence sources” (CHIS).
- 1.2 The legislation was introduced to ensure that individuals’ rights are protected while also ensuring that law enforcement and security agencies have the powers they need to do their job effectively.
- 1.3 RIPA requires that when a Council undertakes “directed surveillance” or uses a CHIS, these activities must be authorised in advance by an officer with delegated powers when the relevant criteria are satisfied and, since November 2012 there has been an additional requirement for approval by a Justice of the Peace.
- 1.4 The Council’s current policy is attached as Appendix A.
- 1.5 The Home Office’s recently issued guidance¹ reaffirms the recommendation that, to attain best practice:

“...elected members of a local authority should review the authority’s use of the 2000 Act and set the policy at least once a year. They should also consider internal reports on use of the 2000 Act on a regular basis to ensure that it is being used consistently with the local authority’s policy and that the policy remains fit for purpose.”

¹ *Guide on Covert Surveillance and Property Interference (2014)*

2.0 Report

Council Policy and Positioning on Surveillance

- 2.1 The Council's policy, entitled "The Regulation of Investigatory Powers Act 2000 – A Working Policy" was originally established in 2000 in response to the legislation and has undergone minor updates since. The latest updates have been made to reflect changes in the Council's management structures and the implications of legislative changes.
- 2.2 The only purpose for which local authorities are able to rely on RIPA is where the authorisation is necessary *"for the purpose of preventing and detecting crime and disorder"*. Additionally, authorisation is now subject to a 'crime threshold test' under which the crime is punishable by a maximum term of at least 6 months imprisonment.
- 2.3 The Council's "statement of intent" as expressed in the policy is:

"The Council's policy and practice in respect of RIPA is to comply fully with the law and strike a fair and proportionate balance between the need to carry out covert surveillance in the public interest and the protection of an individual's fundamental right to privacy. The Council acknowledges that this policy is very much a living document and will be reviewed and updated in line with the best guidance and advice current at the time."

Control and Monitoring

- 2.4 Public bodies are required to formally establish responsibility for approving RIPA authorisations and the Council has set this at Chief Officer level, there being no downward delegation available.
- 2.5 The Chief Officer (Governance) is the Council's designated "Senior Responsible Officer" in relation to RIPA and thereby responsible for the integrity of the Council's processes, compliance with legislation and engagement with the Commissioners and inspectors. The Chief Officer (Governance) is assisted in this role by the Senior Solicitor.
- 2.6 The Internal Audit Manager performs the role of RIPA Co-ordinator, maintaining the required "central record" of authorisations, monitoring the review, renewal and cancellation of authorisations and performing a quality control role on the paperwork.

Recent Activity and Performance

- 2.7 The Council has never authorised the use of a CHIS. Use made of RIPA in recent years to authorise directed surveillance is summarised in the following table:

Purpose of Surveillance	Number of authorisations					
	2009	2010	2011	2012	2013	2014
Alleged Benefit fraud	1	-	-	1	-	-
Alleged noise nuisances – Digital Audio Tape (DAT) recording equipment used	2	-	-	-	-	-
Alleged vehicle damage – CCTV used.	1	-	-	-	-	-
Internal investigation – suspected email abuse	1	-	-	-	-	-
Operation to combat dog fouling	-	-	-	2	-	-
Alleged food standards contravention	-	-	-	-	-	1
Total of Directed Surveillance Authorisations	5	0	0	2	0	1

2.8 The above table demonstrates that the Council has continued to take a measured approach to its use of RIPA.

Results of Inspections (Office of the Surveillance Commissioner OSC)

2.9 The Council has now been visited by an Assistant Surveillance Commissioner on five occasions since the legislation was introduced, most recently on 26th November 2014. A copy of the inspection report is attached as Appendix B.

2.10 It is pleasing to note the extremely positive tone and content of the report. The two recommendations made in the report have been attended to.

3.0 Details of Consultation

3.1 None.

4.0 Conclusion

4.1 Given the positive report received from the Assistant Commissioner and the continuing limited extent to which the Council engages in surveillance Members are asked to note the report and endorse the Council's RIPA Policy.

<p>CONCLUSION OF IMPACT ASSESSMENT (including Diversity, Human Rights, Community Safety, Sustainability and Rural Proofing)</p> <p>Not applicable</p>	
<p>FINANCIAL IMPLICATIONS</p> <p>None directly arising from this report</p>	
<p>SECTION 151 OFFICER'S COMMENTS</p> <p>The Section 151 Officer has been consulted and has no further comments.</p>	
<p>LEGAL IMPLICATIONS</p> <p>None arising from the report.</p>	
<p>MONITORING OFFICER'S COMMENTS</p> <p>The Monitoring Officer has been consulted and has no further comments.</p>	
<p>BACKGROUND PAPERS</p>	<p>Contact Officer: Derek Whiteway Telephone: 01524 582028 E-mail: dwhiteway@lancaster.gov.uk Ref: aud/comm/audit/210115RIPA</p>



THE REGULATION OF INVESTIGATORY POWERS ACT 2000 –

A WORKING POLICY

The Purpose of this Policy

1. The purpose of this policy is to:
 - ❑ explain the provisions of the Regulation of Investigatory Powers Act 2000 (RIPA);
 - ❑ provide guidance and give advice to those Services undertaking covert surveillance; and
 - ❑ ensure full compliance with RIPA and a Council-wide consistent approach to its interpretation and application.

Introduction to RIPA

2. RIPA came into force on 25th September 2000 to regulate covert investigations by a number of bodies, including local authorities. It was introduced to ensure that individuals' rights are protected while also ensuring that law enforcement and security agencies have the powers they need to do their job effectively.

Lancaster City Council is therefore included within the 2000 Act framework with regard to the authorisation of both Directed Surveillance and the use of Covert Human Intelligence Sources (CHIS)

3. In summary RIPA requires that when a Council undertakes "directed surveillance" or uses a "covert human intelligence source" these activities must only be authorised by an officer with delegated powers when the relevant criteria are satisfied. In addition, amendments contained in the Protection of Freedoms Act 2012, which took effect on the 1st November 2012, mean that local authority authorisations, and renewals of authorisations under RIPA, can only take effect once an order approving the authorisation (or renewal) has been granted by a Justice of the Peace (district judge or lay magistrate)(JP).
4. Authorisation for both types of surveillance may be granted only where it is believed that the authorisation is necessary and the authorised surveillance is proportionate to that which is sought to be achieved:

An authorisation may be granted only where the Authorising Officer believes that the authorisation is necessary in the circumstances of the particular case:

"For the purpose of preventing and detecting crime and disorder"

However, amendments which took effect on the 1st November 2012 mean that a local authority may only authorise use of directed surveillance under RIPA to prevent or detect criminal offences that are either punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months' imprisonment or are related to the underage sale of alcohol and tobacco. Local authorities cannot authorise directed surveillance for the purpose of preventing disorder unless this involves a criminal offence punishable by a maximum term of at least 6 months' imprisonment. These amendments are referred to as "the crime threshold".

5. The background to RIPA is the Human Rights Act 1998, which imposes a legal duty on public authorities to act compatibly with the European Convention on Human Rights (ECHR). Article 8(1) of the ECHR gives a right to respect for private and family life, the home and correspondence. However, this is qualified by Article 8(2) which provides that there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. RIPA was enacted so as to incorporate the provisions of Article 8(2) in English law, and to establish a means by which a public authority may interfere with privacy rights in accordance with the law. The objective is to give protection to the Council and any officer involved in an investigation. The scheme of RIPA is to state that an authorisation for covert surveillance shall be lawful for all purposes, but that such an authorisation may only be granted if the authorising officer believes that what is proposed is necessary and proportionate (see paragraphs 35 and 36 below).
6. If the authorisation procedures introduced by RIPA are followed, they afford protection to the Council and to investigating officers in respect of challenges to the admissibility of evidence, claims under the Human Rights Act 1998, and complaints to the Local Government Ombudsman or the Investigatory Powers Tribunal.
7. The Act is supported by statutory Codes of Practice, the most recent versions of which were published in 2014 and are available on the Council's intranet. These are the 'Covert Surveillance and Property Interference' Code of Practice and the 'Covert Human Intelligence Sources' (CHIS) Code of Practice. RIPA requires the Council to have regard to the provisions of the Codes which are admissible as evidence in criminal and civil proceedings and must be taken into account by any court or tribunal.

Office of Surveillance Commissioners

8. In May 2001 an Inspectorate was formed within the Office of Surveillance Commissioners (OSC) to assist the 'Chief Surveillance Commissioner' keep under review the exercise and performance of the powers and duties conferred or imposed by RIPA. The most recent Procedures and Guidance document was issued by the Chief Surveillance Commissioner in December 2014, and is available on the Council's intranet.
9. RIPA requires public authorities to disclose or provide to the Chief Surveillance Commissioner all such documents and information as he may require for the purpose of enabling him to carry out his functions.

Statement of intent

10. The Council's policy and practice in respect of RIPA is to comply fully with the law and strike a fair and proportionate balance between the need to carry out covert surveillance in the public interest and the protection of an individual's fundamental right to privacy. The Council acknowledges that this policy is very much a living document and will be reviewed and updated in line with the best guidance and advice current at the time.

PART 1: AN EXPLANATION OF THE KEY PROVISIONS OF RIPA**What is meant by 'surveillance'?**

11. 'Surveillance' includes:
- a) monitoring, observing or listening to persons, their movements, their conversations or their other activities or communication;
 - b) recording anything monitored, observed or listened to in the course of surveillance; and
 - c) surveillance by or with the assistance of a surveillance device.

When is surveillance 'covert'?

12. According to RIPA, surveillance is covert if, and only if, it is carried out in a manner that is calculated to ensure that persons who are subject to the surveillance are unaware that it is or may be taking place. If activities are open and not hidden from the subjects of an investigation, the 2000 Act framework does not apply.

What is 'directed surveillance' or when is surveillance 'directed'?

13. Surveillance is directed if it is 'covert' but *not* 'intrusive' (see below) and is undertaken:
- a) for the purposes of a specific investigation or a specific operation;
 - b) in such a manner as is likely to result in the obtaining of private information about a person (whether or not that person is specifically identified for the purposes of the investigation or operation); and
 - c) otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation to be sought for the carrying out of the surveillance.

14. Essentially, therefore, directed surveillance is any:
- (1) pre-planned surveillance activity;
 - (2) undertaken covertly;
 - (3) for the purposes of a specific investigation;
 - (4) in such a way that is *likely* to result in obtaining private information about a person.

15. **Is it for the purposes of a specific investigation or operation?**

For example, are CCTV cameras which are readily visible to anyone walking around a Council car park covered?

The answer is not if their usage is to monitor the general activities of what is happening in the car park. If that usage changes at any time the 2000 Act may apply.

For example, if the CCTV cameras are targeting a particular known individual, and are being used in monitoring his activities, that has turned into a specific operation which will require authorisation.

16. **Is it in such a manner that is likely to result in the obtaining of private information about a person?**

‘Private information’ in relation to a person, includes any information relating to his private or family life. Private information should be taken generally to include any aspect of a person’s private or personal relationship with others, including family and professional or business relationships. Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person’s activities in public may still result in the obtaining of private information. This is likely to be the case where that person has a reasonable expectation of privacy even though acting in public and where a record is being made by a public authority of that person’s activities for future consideration.

If it is likely that observations will not result in the obtaining of private information about a person, then it is outside the 2000 Act framework. However the use of “test purchasers” may involve the use of covert human intelligence sources (see para 92)

17. **‘Immediate response....’**. According to the Covert Surveillance Code of Practice, “covert surveillance that is likely to reveal private information about a person but is carried out by way of an immediate response to events such that it is not reasonably practicable to obtain an authorisation under the 2000 Act would not require a directed surveillance authorisation.” For example, a police officer would not require an authorisation to conceal himself and observe a suspicious person that he came across in the course of a patrol.

However, if as a result of an immediate response, a specific investigation subsequently takes place, that brings it within the 2000 Act framework.

18. **What is meant by ‘intrusive surveillance’ or when is surveillance ‘intrusive’?**

Surveillance becomes intrusive if the covert surveillance :

- a) is carried out in relation to anything taking place on any **'residential premises'** or in any **'private vehicle'**; or a **"place for legal consultation"**; and
- b) involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device; or
- c) is carried out by means of a surveillance device in relation to anything taking place on any residential premises or in any private vehicle but is carried out without that device being present on the premises or in the vehicle, and the device is such that it **consistently provides information of the same quality and detail** as might be expected to be obtained from a device actually present on the premises or in the vehicle.

The definition of surveillance as intrusive relates to the location of the surveillance, and not to other consideration of the nature of the information that is expected to be obtained. Officers of the Council are unlikely to have access to any "place of legal consultation", but should seek advice from legal Services on the detailed definition.

- 19. **'Residential premises'** is defined to include any premises that is for the time being occupied or used by any person, however temporarily, for residential purposes or otherwise as living accommodation. For example, the definition includes hotel rooms. It, however, does not include so much of any premises as constitutes any common area to which a person is allowed access in connection with his use or occupation of any accommodation. For example, a hotel lounge.
- 20. **'Private vehicle'** means any vehicle which is used primarily for private purposes, for example, for family, leisure or domestic purposes. It therefore does not include taxis i.e. private hire or hackney carriage vehicles.

Why is it important to distinguish between directed and intrusive surveillance?

- 21. It is imperative that officers understand the limits of directed surveillance or, put another way, recognise when directed surveillance becomes intrusive surveillance because **RIPA does not permit local authorities to undertake intrusive surveillance in any circumstances.**

What is a 'covert human intelligence source' (CHIS)?

- 22. According to RIPA a person is a CHIS if:
 - a) he **establishes or maintains a personal or other relationship** with a person for the **covert purpose** of facilitating the doing of anything falling within paragraph b) or c).
 - b) he covertly uses such a relationship to **obtain information** or provide access to any information to another person; or
 - c) he covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

23. A CHIS is effectively an inside informant or undercover officer, someone who develops or maintains their relationship with the surveillance target, having the covert purpose of obtaining or accessing information for the investigator.
24. A **purpose is covert**, in relation to the establishment or maintenance of a personal or other relationship, if and only if the relationship is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose.
25. It is not clear whether '**information**' is restricted to private information in line with directed surveillance. The inference is there, but it is not clear. If in doubt, the Council's policy is to obtain an authorisation.
26. RIPA also makes reference to the use of a CHIS which refers to inducing, asking or assisting a person to engage in the conduct of a CHIS, or to obtain information by means of the conduct of such a CHIS.

PART 2: GENERAL AUTHORISATION REQUIREMENTS

The authorisation requirements

27. RIPA requires that prior authorisation is obtained by all local authorities using directed surveillance and CHIS techniques.
28. The authorising officer must give authorisations in writing and a separate authorisation is required for each investigation. Any authorisation must also be approved by an order from a JP. The application form for such approval is available on the Council's intranet, but advice should be sought from Legal Services on making an application for judicial approval.
29. Whilst according to RIPA, a single authorisation may combine two or more different authorisations (for example, directed surveillance and CHIS), the provisions applicable in the case of each of the authorisations must be considered separately. Because combining authorisations may cause confusion, officers must use separate forms for different authorisations.
30. The purpose of the authorisation is to comply with the Human Rights Act 1998 by providing lawful authority to carry out surveillance. This is why an authorisation must be obtained where the surveillance is likely to interfere with a person's Article 8 rights to privacy by obtaining private information about that person, whether or not that person is the subject of the investigation or operation. If the surveillance is then actually carried out in accordance with the authorisation, it will be less open to challenge.

Who can authorise the use of covert surveillance?

31. To give effect to RIPA, (1) **Chief Officers** have been designated to authorise the use of directed surveillance and CHIS techniques in respect of external investigations and (2) **the Monitoring Officer** is authorised to sanction the use of such covert surveillance in respect of internal officer/Member investigations. Any RIPA authorisation must be approved by an order from a JP. The JP will be provided with a copy of the authorisation, and with a partially completed judicial application/order form, which is available on the

Council's intranet. Advice should be sought from Legal Services, who will contact the court to arrange the hearing date for the application.

32. It should also be noted that in accordance with the relevant Regulations, the designation of Chief Officers to sanction the use of RIPA regulated covert surveillance extends upwards to the Chief Executive. This is in accordance also with the Council's own Constitution.
33. Ideally, authorising officers should not be responsible for authorising their own activities i.e. those operations/investigations in which they are directly involved. However, the Codes of Practice recognise that this may sometimes be unavoidable, especially in the case of small organisations, or where it is necessary to act urgently.

Justification for covert surveillance

34. In order to use covert surveillance (both directed surveillance and a CHIS) lawfully the person granting the authorisation (i.e. the authorising officer) will have to demonstrate that the surveillance is both '**necessary**' and '**proportionate**' to meet the objective of the prevention or detection of crime or of prevention of disorder. The JP must also be satisfied that the use of the technique is necessary and proportionate.

The necessity test

35. RIPA first requires that the authorising officer must be satisfied that the authorisation is necessary, in the circumstances of the particular case, for the prevention and detection of crime, or prevention of disorder. This is the only statutory ground on which local authorities are now able to carry out directed surveillance and use a CHIS. For the purposes of the authorisation of directed surveillance, the crime threshold referred to in paragraph 4 above must be met. Covert surveillance cannot be "necessary" unless, in that particular case, there is no reasonably available overt method of discovering the desired information.

The proportionality test

36. Then, if the activities are necessary, the authorising officer must be satisfied that they are proportionate to what is sought to be achieved by carrying them out. This involves balancing the intrusiveness of the activity on the target and others who might be affected by it against the need for the activity in operational terms. The activity will not be proportionate if it is **excessive** in the circumstances of the case or if the information which is sought could reasonably be obtained by other less intrusive means. All such activity should be carefully managed to meet the objective in question and must not be arbitrary or unfair.

CHIS – additional requirements

37. In addition, there are further criteria in relation to CHIS authorisations. Namely, that specific arrangements exist to ensure that, amongst other things, the source is independently managed and supervised, that records are kept of the use made of the source, that the source's identity is protected from those who do not need to know it, and that arrangements also exist to satisfy such other requirements as may be imposed by an Order made by the Secretary of State.

38. RIPA provides that an authorising officer must not grant an authorisation for the use or conduct of a source unless he believes that arrangements exist that satisfy these requirements. In this regard, the particular attention of authorising officers is drawn to paragraph 6.14 of the CHIS Code of Practice concerning the security and welfare of a CHIS and the need to carry out a **risk assessment**.
39. ***The Regulation of Investigatory Powers (Source Records) Regulations 2000 (SI No. 2725)*** details the particulars that must be included in the records relating to each CHIS. The authorising officer should comment on all these aspects in his “comments” box, as he may have to justify the fact that he has taken account of these requirements and made an appropriate provision to comply.

Collateral Intrusion

40. Before authorising surveillance the authorising officer should also take into account the risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation or operation (particularly when considering the proportionality of the surveillance). This is referred to as collateral inclusion, and the following should be considered::
- I. measures should be taken, wherever practicable, to avoid or minimise unnecessary intrusion into the privacy of those not directly connected with the investigation or operation;
 - II. an application for an authorisation should include an assessment of the risk of any collateral intrusion and the authorising officer should take this into account, when considering the proportionality of the surveillance;
 - III. those carrying out the surveillance should inform the authorising officer if the investigation or operation unexpectedly interferes with the privacy of individuals who are not covered by the authorisation; and
 - IV. when the original authorisation may not be sufficient, consideration should be given to whether the authorisation needs to be amended and reauthorised or a new authorisation is required.

Local community ‘sensitivities’

41. Any person applying for or granting an authorisation will also need to be aware of what the Codes of Practice refer to as “*any particular sensitivities in the local community*” where the surveillance is taking place or of similar activities being undertaken by other public authorities which could impact on the deployment of surveillance.

PART 3: DIRECTED SURVEILLANCE AUTHORISATION REQUIREMENTS

Applications for directed surveillance authorisation

42. Applications for authorisation to carry out directed surveillance must be made in **writing** using the **standard Application Form** and judicial approval form available on the Council’s intranet.

Duration of directed surveillance authorisations

43. A written authorisation granted by an authorising officer, and approved by a JP, will cease to have effect (unless renewed) at the end of a period of **three months** beginning with the day on which it took effect.

Reviews of directed surveillance authorisations

44. Regular reviews of authorisations should be undertaken to assess the need for the surveillance to continue. Particular attention is drawn to the need to review authorisations frequently where the surveillance provides access to '**confidential information**' (see below) or involves collateral intrusion.
45. Authorisations must be reviewed by the authorising officer therefore **at least monthly** using the **standard Review Form** available on the Council's intranet to ensure that they remain in force only for so long as it is necessary.

Renewals of directed surveillance authorisations

46. If at any time before an authorisation would cease to have effect, the authorising officer considers it necessary for the authorisation to continue for the purpose for which it was given, he may renew it in writing **for a further period of three months** using the **standard Renewal Form** available on the Council's intranet. The same conditions attach to a renewal of surveillance as to the original authorisation. An order from a JP is required for a renewal in the same way as for an authorisation.
47. A renewal takes effect at the time at which, or day on which the authorisation would have ceased to have effect but for the renewal. An application for renewal should not be made until **10 working days** before the authorisation period is drawing to an end. However, where renewals are timetabled to fall outside of court hours, for example during a holiday period, care must be taken to ensure that the renewal is completed ahead of the deadline.
48. Any person who would be entitled to grant a new authorisation can renew an authorisation, but an order from a JP is also required.. Authorisations may be renewed more than once, provided they continue to meet the criteria for authorisation.

Cancellation of directed surveillance authorisations

49. The authorising officer who granted or last renewed the authorisation **must** cancel it using the **standard Cancellation Form** available on the Council's intranet if he is satisfied that the directed surveillance no longer meets the criteria upon which it was authorised. Authorisations should not be allowed to simply expire.
50. Where the authorising officer is no longer available, this duty will fall on the person who has taken over the role of authorising officer or the person who is acting as authorising officer (*see the Regulation of Investigatory Powers (Cancellation of Authorisations) Order 2000; SI No: 2794*).
51. If the authorising officer is on sick or annual leave or is otherwise unable to cancel the authorisation for good reason, any other officer designated to grant authorisations may cancel the authorisation.

Ceasing of surveillance activity

52. As soon as the decision is taken that directed surveillance should be discontinued, the instruction must be given to those involved to stop all surveillance of the subject(s). The date and time when such an instruction was given should be recorded in the notification of cancellation where relevant (see standard cancellation form).

Urgent cases

53. A JP may consider an authorisation out of working hours in exceptional cases. This must be arranged through the court, and two completed judicial application/order forms must be provided so that one can be retained by the JP.

Confidential information

54. RIPA does not provide any special protection for '**confidential information**'. The Codes of Practice, however, do provide additional safeguards for such information. Confidential information consists of matters subject to **legal privilege**; **confidential personal information** (information relating to the physical or mental health or spiritual counselling of a person who can be identified from it) or **confidential constituent information** (relating to communications between a Member of Parliament and a constituent in respect of constituency matters) or **confidential journalistic material** (material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence). Further details about these categories of confidential information are set out in the Codes themselves, and advice can be obtained from Legal Services.
55. Special care should be taken if there is a likelihood of acquiring any confidential information. Such authorisations should only be granted in exceptional and compelling circumstances with full regard to the proportionality issues such surveillance raises.
- 56.. In accordance with the provisions of the Code, in cases where through the use of the surveillance it is likely that confidential information will be acquired, the use of surveillance must be authorised by the **Chief Executive**.
57. If, exceptionally, any Council investigation is likely to result in the acquisition of confidential material, officers are required to **obtain the prior approval of Legal Services** before applying for an authorisation.
58. If confidential material is acquired during the course of an investigation, the following general principles apply:
- confidential material should not be retained or copied unless it is necessary for a lawful purpose;
 - confidential material should be disseminated only where an officer (having sought advice from the Legal Services Manager) is satisfied that it is necessary for a lawful purpose;
 - the retention or dissemination of such information should be accompanied by a clear warning of its confidential nature. It should be safeguarded by taking reasonable steps to ensure that there is no possibility of it becoming

- available, or its content being known, to any person whose possession of it might prejudice any criminal or civil proceedings related to the information; and
- confidential material should be destroyed as soon as it is no longer necessary to retain it for a specified purpose.

PART 4: CHIS AUTHORISATION REQUIREMENTS

59. Generally speaking, the authorisation requirements for directed surveillance also apply to a CHIS authorisation. There are, however, some variations, and the crime threshold as set out in paragraph 4 does not apply to a CHIS authorisation.

Duration of CHIS authorisations

60. A written CHIS authorisation granted by an authorising officer and approved by a JP, will cease to have effect (unless renewed) at the end of a period of **twelve months** beginning with the day on which it took effect.

Renewal of CHIS authorisations

61. An authorising officer may renew a CHIS authorisation in writing **for a further period of twelve months**. This is subject to approval from a JP.
62. The same conditions attach to a renewal of surveillance as to the original authorisation. However, before renewing an authorisation for the use or conduct of a CHIS, officers are required to carry out a review of the use made of that source, the tasks given to that source and the information so obtained.

CHIS forms

63. Standard **CHIS Application; Review; Renewal, and Cancellation Forms, and the Judicial Approval form** are available on the Council's intranet. Officers are required to use these forms in the appropriate circumstances.

Vulnerable individuals

64. In accordance with the CHIS Code of Practice, a '**vulnerable person**' should only be authorised to act as a CHIS in the most exceptional circumstances and must be authorised by the **Chief Executive**. Legal advice should always be sought. A 'vulnerable individual' is a person who is or may be in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take care of himself, or unable to protect himself against significant harm or exploitation.

Juvenile sources

65. Special safeguards also apply to the use or conduct of juvenile sources; that is sources under the age of 18 years. Legal advice should always be sought. On no occasion should the use or conduct of a CHIS under 16 years of age be authorised to give information against his parents or any person who has parental responsibility for him. In other cases, authorisations should not be granted unless the special provisions contained within ***The Regulation of Investigatory Powers (Juveniles) Order 2000 (SI No. 2793)*** are satisfied. Authorisations for juvenile sources must be authorised by the **Chief**

Executive The duration of such an authorisation is **one month only** instead of the usual twelve months.

PART 5: OTHER AUTHORISATION REQUIREMENTS

Central Record of all authorisations

66. The Codes of Practice provide that a centrally retrievable record of all authorisations should be held by each public authority and regularly updated whenever an authorisation is granted, reviewed, renewed or cancelled. The record should be made available to the relevant Commissioner or an Inspector from the Office of Surveillance Commissioners (OSC), upon request. These records will be retained for a period of at least three years from the ending of the authorisation and will comprise of the information prescribed in the Codes.
67. The Council will also maintain a record of specified documentation relating to authorisations as further required by the Codes.
68. To give effect to these requirements Internal Audit have set up, and will maintain, a central recording and monitoring system. **Authorising officers are required to e-mail all completed RIPA forms to Internal Audit within two working days** of the grant; review; renewal; or cancellation of the authorisation so that the Council's central recording and monitoring systems can be kept up to date. **Authorising officers are also required to send a copy of all RIPA forms to the Head of Governance, as Monitoring Officer** so that a central register of RIPA forms can be maintained.
69. Authorising officers should however ensure that original RIPA forms are kept on the investigation case file and stored securely.
70. To assist Services, Internal Audit has set up an e-mail alert facility for authorisations. That is, Internal Audit will e-mail authorising officers 14 days before an authorisation is due to expire reminding them to either renew the authorisation if it is necessary for the surveillance to continue or to cancel the authorisation by completing the appropriate form.
71. In addition, the **Monitoring Officer** will receive **periodic status reports** from Internal Audit to enable her to be satisfied that RIPA authorisation requirements are being complied with.

Retention and destruction of the product of surveillance

72. Where the product of surveillance could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with established disclosure requirements for a suitable period, commensurate to any subsequent review.
73. The Codes of Practice draw particular attention to the requirements of the code of practice issued under the **Criminal Procedure and Investigations Act 1996**. This requires that material which is obtained in the course of a criminal investigation and which may be relevant to the investigation must be recorded and retained.

- 74 Where material is obtained by surveillance, which is **wholly unrelated** to a criminal or other investigation or to any person who is the subject of the investigation, and there is no reason to believe it will be relevant to future civil or criminal proceedings, it should be **destroyed immediately**. Consideration of whether or not unrelated material should be destroyed is the responsibility of the authorising officer.
75. There is nothing in RIPA which prevents material obtained from properly authorised surveillance from being used in other investigations. Each Service must ensure that arrangements are in place for the handling, storage and destruction of material obtained through the use of covert surveillance. Authorising officers must ensure compliance with the appropriate data protection requirements relating to the handling and storage of material.

Acting on behalf of another

- 76 In cases where one agency is acting on behalf of another, it is usually for the tasking agency to obtain or provide the authorisation. For example, where surveillance is carried out by the Police with the use of the Council's CCTV systems, an authorisation must be obtained by the Police.

PART 6: PRACTICAL APPLICATION OF RIPA

Who is affected by RIPA?

77. As the Council has already recognised in respect of the application of the **Human Rights Act 1998**, RIPA will impact on the enforcement activities of all the Council's regulatory Services, but, in the case of authorisations for directed surveillance, the crime threshold referred to in paragraph 4 must be met. This means that directed surveillance will no longer be able to be used in some investigations where it was previously authorised, eg dog fouling. However, this does not mean that it will not be possible to investigate these matters with a view to stopping offending behaviour. Routine patrols, observation at trouble "hotspots", immediate response to events and overt use of CCTV are all techniques which do not require RIPA authorisation.

A public authority may only engage RIPA when in performance of its "core functions" in contrast to the "ordinary functions" which are undertaken by all authorities (eg employment and contractual matters). Accordingly, the disciplining of an employee is not a core function, although related criminal investigations may be.

'general observation vs. 'systematic surveillance'

78. According to the Covert Surveillance Code of Practice "General observation duties of many law enforcement officers and other public authorities do not require authorisation under the 2000 Act". For example, police officers will be on patrol to prevent and detect crime, maintain public safety and prevent disorder or trading standards or HM Customs and Excise officers might covertly observe and then visit a shop as part of their enforcement function to verify the supply or level of supply of goods or services that may be liable to a restriction or tax. Such observation may involve the use of equipment to merely reinforce normal sensory perception, such as binoculars, or the use of cameras, where this does not involve systematic surveillance of an individual.

79. The clear view expressed therefore is that usually low-level activity such as general observation will **not** be regulated under the provisions of RIPA provided it does not involve the systematic surveillance of an individual. That said, the determination of what constitutes 'general observation' on the one hand and 'systematic surveillance' on the other is a question of fact, the determination of which is not always straightforward and depends on the particular circumstances of an individual case.
80. In practice, the issue will turn on whether the covert surveillance is *likely* to result in obtaining any information in relation to a person's private or family life, whether or not that person is the target of the investigation or operation. If in doubt you are strongly recommended to obtain an authorisation.

'covert' vs. 'overt' surveillance

81. In accordance with the Council's usual practice, wherever possible and appropriate Services should give advance warning of their intention to carry out surveillance. This is because the provisions of RIPA regulate the use of covert surveillance only. In some cases a written warning may itself serve to prevent the wrongdoing complained of.
82. However, in order to properly put a person on notice that he is or may be the subject of surveillance, the notification letter must be couched in sufficiently precise terms so that he knows what **form** the surveillance will take (i.e. record of noise; photographs etc.). In fact, in line with directed surveillance requirements, notification letters should state **how long** the surveillance is likely to last (which should not be longer than three months); the necessity for the surveillance should be **reviewed at least monthly**; if it is necessary to continue the surveillance beyond the initial specified period a **renewal letter** should be sent to the 'noisy' neighbour, for example, and he should be informed when the surveillance has ceased.
83. It is also important to instruct the investigating officer not to exceed the limits of the 'surveillance' he has been asked to carry out.
84. Whilst it is accepted that the definition of 'covert' set out in RIPA could be interpreted very broadly, it is suggested that whether the surveillance activity is covert or not depends on the investigator's intention and conduct. If there is some element of **secrecy** or **concealment** the activity is likely to be covert.
85. Wherever possible or appropriate, officers should be **open; obvious and overt**.

CCTV

- 86 Overt CCTV systems used for general purposes are **not** usually regulated by RIPA (but CCTV in general is regulated by the **Data Protection Act 1998** and the **CCTV Code of Practice** issued by the Office of the Information Commissioner). If, however, CCTV systems are used to **track individuals** or **specific locations** and the surveillance is pre-planned (i.e. not an immediate response to events or circumstances which by their very nature, could not have been foreseen) a **directed surveillance** authorisation must be obtained.

Recognising a CHIS

- 87.. The provisions of RIPA are not intended to apply in circumstances where members of the public volunteer information to the police or other authorities, as part of their normal civic duties, or to contact numbers set up to receive information (such as Crimestoppers, Customs Confidential, the Anti Terrorist Hotline, or the Security Service Public Telephone Number). Members of the public acting in this way would not generally be regarded as sources.
88. However, when an informant gives repeat information about a suspect or about a family, and it becomes apparent that the informant may be obtaining the information in the course of a family or neighbourhood relationship, this probably means that the informant is a CHIS, to whom a duty of care is owed if the information is then used, even though he or she has not been tasked by the authority to obtain information on its behalf.
- 89 The use of professional witnesses to obtain information and evidence is clearly covered.

“.....establishing or maintaining a personal or other relationship.....”

- 90 Whilst the meaning of “...establishing or maintaining a personal or other relationship...” is not clear and is open to interpretation, it is suggested that there has to be some measure of **intimacy** beyond the ordinary conversation. Only if an officer, for example, establishes some measure of **trust and confidence** with the person who is the subject of the surveillance will he be establishing or maintaining a personal or other relationship.
- 91 Usually a simple enquiry or a request for general information (i.e. a request for information which would be supplied to any member of the public who enquired) *not* obtained under false pretences is not likely to be regulated by RIPA.

Simple test purchase transactions

92. Whether or not test purchase transactions are regulated by RIPA depends on the circumstances and in particular the conduct of the person carrying out the surveillance. Usually simple covert test purchase transactions carried out under existing statutory powers where the officer involved does not establish a personal or other relationship will not require a CHIS authorisation.
93. Officers should, however, be wary of the law on **‘entrapment’**. Whereas officers can in appropriate circumstances, present a seller or supplier, for example, an opportunity which he could act upon, officers cannot ‘incite’ the commission of an offence i.e. encourage, persuade or pressurise someone to commit an offence.

Use of DAT recorders

94. If it is appropriate to do so, Environmental Health officers, and to a much lesser extent Council Housing officers, use a recorder to monitor noise levels (usually at residential premises) following noise nuisance complaints. Whilst the recorder is installed by officers, the complainant decides when to switch the recorder on and off.
95. The covert recording of suspected noise nuisance where the intention is only to record excessive noise levels from adjoining premises, and the recording device is calibrated to record only excessive noise levels, may not require an

authorisation, as the perpetrator would normally be regarded as having forfeited any claim to privacy

96. That said, a Digital Audio Tape (DAT) recorder is a sophisticated piece of monitoring equipment and if used covertly may constitute directed surveillance. In general, a letter is sent to the person who is to be the subject of the surveillance, and this should mean that subsequent surveillance is overt, and an authorisation will not as a matter of course be required. However, if there is any doubt as to whether surveillance is covert, eg if any longer than a few weeks has passed since the alleged perpetrator was informed that monitoring might be carried out, and if it is likely that private information will be obtained, then an authorisation should be sought.

RIPA forms

97. It is imperative that RIPA forms are completed in full whenever RIPA regulated surveillance activity is planned. The information given must be specific and detailed; must relate to the particular facts of an individual case (i.e. avoid standard wording if at all possible) and must demonstrate that a proper risk assessment has been carried out. Both those who apply for an authorisation and the Authorising Officer should refer to this policy and to the relevant Code of Practice in completing the relevant form,

Role of Chief Officers/Authoring Officers

98. Chief Officers in particular must recognise that RIPA imposes new and important obligations on those Services affected by RIPA.
99. Authorising officers are required to ask themselves: "Have I got sufficient information to make an informed decision as to whether or not to authorise surveillance activity on the particular facts of this case?"
100. Authorising officers must be satisfied that there are adequate checks in place to ensure that the surveillance carried out is in line with what has been authorised. Such monitoring should be properly documented as well as the decision making process in general.
101. Officers are strongly recommended to read this policy in conjunction with the Covert Surveillance and CHIS Codes of Practice which provide supplementary guidance.
102. If the surveillance is not properly authorised, the protection offered by RIPA will be lost.

How to access RIPA documents?

103. RIPA itself; explanatory notes to RIPA, the Covert Surveillance and CHIS Codes of Practice; RIPA statutory instruments and other RIPA documents are available on the Home Office web-site:
www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers/.
104. Relevant RIPA documents as well as this policy and the Council's standard forms have also been posted on the Council's intranet.



Office of Surveillance
Commissioners



Chief
Surveillance
Commissioner

OFFICIAL - SENSITIVE

17th December 2014

Dear Mr. Cullinan,

Covert Surveillance

On 26th November 2014, an Assistant Surveillance Commissioner, HH David Hodson, visited your Council on my behalf to review your management of covert activities. I am grateful to you for the facilities afforded for the inspection.

I enclose a copy of Mr Hodson's report which I endorse. It is over 50 years since, as a young barrister, I first appeared in the old Magistrates Court in Lancaster Town Hall, to which Mr Hodson refers in paragraph 7 of his report; and it is at about the same time that my late father retired as Town Clerk of Morecambe. Much legislation has flowed under the bridge since then, of which RIPA is for present consideration. I am very pleased to see that Mr Hodson describes your officers as 'second to none in their dedication, experience, expertise and professionalism'. Your processes and practices are generally RIPA compliant and some errors can readily be addressed.

The two recommendations are that your Central Record be amended as indicated in paragraph 13 of the report and that the frailties exposed in paragraph 14 be addressed by refresher training.

I shall be glad to learn that your Council accepts the recommendations and will see that they are implemented. One of the main functions of review is to enable public authorities to improve their understanding and conduct of covert activities. I hope your Council finds this process constructive. Please let this office know if it can help at any time.

*Yours sincerely,
Christopher Rose*

Mark Cullinan
Chief Executive
Lancaster City Council
Town Hall
Dalton Square
Lancaster LA1 1PJ

OFFICIAL - SENSITIVE



Office of Surveillance
Commissioners

OFFICE OF SURVEILLANCE COMMISSIONERS

INSPECTION REPORT

Lancaster City Council

26th November 2014

**Assistant Surveillance Commissioner:
HH David Hodson.**

OFFICIAL - SENSITIVE

OFFICIAL- SENSITIVE

DISCLAIMER

This report contains the observations and recommendations identified by an individual surveillance inspector, or team of surveillance inspectors, during an inspection of the specified public authority conducted on behalf of the Chief Surveillance Commissioner.

The inspection was limited by time and could only sample a small proportion of covert activity in order to make a subjective assessment of compliance. Failure to raise issues in this report should not automatically be construed as endorsement of the unreported practices.

The advice and guidance provided by the inspector(s) during the inspection could only reflect the inspectors' subjective opinion and does not constitute an endorsed judicial interpretation of the legislation. Fundamental changes to practices or procedures should not be implemented unless and until the recommendations in this report are endorsed by the Chief Surveillance Commissioner.

The report is sent only to the recipient of the Chief Surveillance Commissioner's letter (normally the Chief Officer of the authority inspected). Copies of the report, or extracts of it, may be distributed at the recipient's discretion but the version received under the covering letter should remain intact as the master version.

The Office of Surveillance Commissioners is not a public body listed under the Freedom of Information Act 2000, however, requests for the disclosure of the report, or any part of it, or any distribution of the report beyond the recipients own authority is permissible at the discretion of the Chief Officer of the relevant public authority without the permission of the Chief Surveillance Commissioner. Any references to the report, or extracts from it, must be placed in the correct context.

OFFICIAL – SENSITIVE



Office of Surveillance
Commissioners

The Rt. Hon Sir Christopher Rose
Chief Surveillance Commissioner
Office of Surveillance Commissioners
PO Box 29105
London SW1V 1ZU

2 December 2014

**LANCASTER CITY COUNCIL
INSPECTION REPORT**

Inspection Date 26 November 2014
Inspector His Honour David Hodson
 Assistant Surveillance Commissioner

Introduction

1. I suppose it was just mere chance that found a Lancastrian Assistant Surveillance Commissioner visiting his old county town on the day before "Lancashire Day" was due to be celebrated. I have to confess that I was unaware that such a red letter day was in the calendar. But there it is, 27 November. The Lancashire Day Proclamation is read out by town criers throughout the county to give Lancastrians the opportunity to declare how proud they are to be Lancastrians. How long it has been celebrated I do not know but, apparently, it commemorates the day in 1295 when Lancashire sent its first representatives to Parliament to form what later became to be called "The Model Parliament."
2. As you will know well, Lancaster City Council is situated in the north-west corner of Lancashire bordering Cumbria to the north and to the east North Yorkshire. It covers approximately 222 square miles and includes the city of Lancaster and the towns of Morecambe and Carnforth. There is a large rural hinterland with a host of villages and hamlets. The population is approximately 135,000 and the Council has a staff of about 880.
3. The senior management structure consists of the Chief Executive with five Chief Officers respectively of Environmental Services, Governance, Health and Housing Services, Regeneration and Planning

1

and Resources. Supporting those Chief Officers are 20 Service Managers.

4. Mr Mark Cullinan remains Chief Executive and his address for correspondence is The Town Hall, Dalton Square, Lancaster LA1 1PJ.
5. The RIPA officers, veterans now of several previous inspections, are Mrs Sarah Taylor, Chief Officer, Governance, who is Senior Responsible Officer and Mr Derek Whiteway, Internal Audit Manager, who is RIPA Co-Ordinating Officer. Authorising Officers are the Chief Officers of the four other departments.
6. During the inspection period there were but three authorisations for Directed Surveillance, two for dog-fouling in March and September 2012 and one for an alleged benefits fraud in October 2012. None involved the obtaining of confidential information or the deployment of a CHIS and no application was refused.

The Inspection

7. I was warmly greeted by Mr Whiteway who immediately introduced me to Mrs Taylor. We had our meeting in what had been the Magistrates' retiring room and I was shown the old court room, long since put out to grass but still obviously a court room with its fine oak furnishings.
8. This Council has won many plaudits in previous inspections and all that I had read in the material that had been sent to me in advance of the inspection led me to expect that this would prove to be yet again a successful inspection.
9. In his report of the previous inspection Sir David Clarke made two recommendations. Firstly, he suggested that the "change of circumstances" form, and all references to it in the Policy, Mini Guides and training materials be dispensed with. That has been done. Sir David also recommended (in paragraph 18) that the Working Policy document be amended to clarify the position where an informant gives repeat information about a suspect or a family so that he may probably be a CHIS. Again this has been done in paragraph 88 of the current version of the Policy with Sir David's words almost jumping off the page.
10. We had an interesting and wide-ranging discussion on RIPA matters generally. It was remarked that the advent of the crime threshold meant that two of the three authorisations I was examining would not now be

possible and that before much longer the DWP would itself be investigating alleged benefit frauds. Consequently it was envisaged that there would be even fewer authorisations in the future. Nonetheless it was fully appreciated that the Council needed to keep its processes and training up to date. Given the experience, expertise and enthusiasm of these RIPA officers I have no doubt that will happen. The pride they have in what they do is almost palpable.

The Council's "A Working Policy"

11. The current edition of this admirable document is dated June 2013 and, as previously, is the work of Mr Whiteway. Again he is to be commended on the excellence of his work not only in the Policy document itself but in the five "RIPA Surveillance Mini Guides" all of which are available on the Intranet. A very helpful feature is the colour coded links to source material.

12. It is most unusual for an Assistant Surveillance Commissioner or an Inspector not to be able to highlight some aspect – however minor - of a Council's policy document that needs amendment. So far as this Council is concerned I have no suggestions for any amendments at all. I was, however, able to point out (for the benefit in due course of paragraph 8) that a new OSC Procedures and Guidance was imminent.

The Central Record.

13. This electronic database designed by Mr Whiteway has been commented upon very favourably in previous inspection reports. I repeat those remarks and would only suggest that the section headed "Authorised by urgent procedure" may be removed and that space be found to record the date when judicial approval is given.

See Recommendation

Examination of the Forms for Directed Surveillance.

14. I examined all three forms for Directed Surveillance. Points arising from numbers 69 and 70 are as follows:

- Number 69. In the cancellation form at paragraph 4 there is confusion. Including the end date of the authorisation in that box is misleading and not necessary. The details as to when the surveillance ceased do not accord with the detail set out in paragraph 2. Further, there is approximately three weeks' delay between the cancellation of the surveillance and the date of the actual cancellation of the authorisation.
- In number 70 the form carries no authorisation URN. The Authorising Officer does not adequately set out why the proposed surveillance is proportionate. She seems to be saying that because the surveillance is necessary it is *therefore* proportionate. There was a delay of approximate *seven* months between the end of the surveillance and the cancellation of the authorisation.
- By way of contrast the forms in number 71 which included two reviews were a perfect example of how these forms should be completed. Necessity and proportionality were covered appropriately. The duration of the authorisation was properly set. Review dates were identified and adhered to. Cancellation was timely and properly recorded. The Authorising Officer responsible for this excellent piece of work was Mrs Taylor and I was able to congratulate her personally. Indeed, so overwhelmed was I with what she had done that I failed to remind her that, ideally, SROs should not generally act as Authorising Officers!

See Recommendation

Training.

15. The Council relies heavily on the on-line Mini Guides amplified if necessary on a case specific basis with advice from either the SRO, Mr Whiteway or the Senior Solicitor, Ms Angela Parkinson. The SRO attended refresher training run jointly with Fylde Borough Council and delivered by Act Now in July 2013 and July 2014. It is felt that this approach is more effective than more formalised training courses for larger groups.

CCTV.

16. Mrs Taylor, Mr Whiteway and I were joined by Mr Mark Davies, Chief Officer, Environmental Services, to discuss the position with regard to CCTV. The basic picture is that the Council does not use their CCTV systems for any covert surveillance activity. Council owned cameras are located in the centres of Lancaster, Morecambe and on two estates. These are used overtly and are, in fact, fairly old and quite primitive. They are analogue and a review as to whether they should be up-dated or replaced is currently under way. The operators had previously been employed by Remploy but the same staff are now employed by Enigma. The same person – previously an officer of HM Customs and Excise – spoken of in Sir David's report is the Supervisor. He is still, I was informed, as robust as ever whenever the Police come to him with their own RIPA authorisations. He ensures that there is no covert use of the CCTV systems without proper RIPA authorisation. Any covert use of the CCTV system is in accordance with the well established agreed protocols.

Conclusion

17. This was the successful inspection that I had expected. The Council's RIPA officers are second to none in their dedication, experience, expertise and professionalism. Their processes and practice are generally RIPA compliant although it is true that some errors were discovered in two forms. These, I am sure can be addressed in specific training. "A Working Policy" is a first rate document and the RIPA Mini Guides are little masterpieces.

18. It is unlikely that RIPA activity will increase much in the near future. Should it do so this Council with this stable RIPA team still in post will be more than able to satisfactorily handle anything that comes their way.

Recommendations

1. That the Central Record be amended to cover the suggestions made in paragraph 13 above.
2. The frailties exposed in paragraph 14 above be addressed in refresher training.

His Honour David Hodson
Assistant Surveillance Commissioner