



## Audit and Risk Management Committee

**Date:** THURSDAY, 17 SEPTEMBER 2015  
**Time:** 1.45 pm  
**Venue:** COMMITTEE ROOMS, 2ND FLOOR, WEST WING, GUILDHALL

**Members:**

Alderman Nick Anstee (Chairman)	Alderman & Sheriff Timothy Hailes
Alderman Charles Bowman	Alderman Ian Luder
Deputy Roger Chadwick (Ex-Officio Member)	Kenneth Ludlam (External Member)
Hilary Daniels (External Member)	Caroline Mawhood (External Member)
Revd Dr Martin Dudley	Jeremy Mayhew (Ex-Officio Member)
Deputy Jamie Ingham Clark	Graeme Smith
Oliver Lodge	Henry Colthurst (Ex-Officio Member)
Alderman Timothy Hailes	Roger Chadwick (Ex-Officio Member)
Alderman Ian Luder	
Graeme Smith	

**Enquiries:** Julie Mayer  
tel. no.: 020 7332 1410  
[julie.mayer@cityoflondon.gov.uk](mailto:julie.mayer@cityoflondon.gov.uk)

**Lunch will be served in Guildhall Club at 1pm**  
**NB: Part of this meeting could be the subject of audio or video recording**

**John Barradell**  
Town Clerk and Chief Executive

# AGENDA

## Part 1 - Public Agenda

1. **APOLOGIES**
2. **MEMBERS' DECLARATIONS UNDER THE CODE OF CONDUCT IN RESPECT OF ITEMS ON THE AGENDA**
3. **MINUTES OF THE PREVIOUS MEETING**  
To agree the public minutes and non-public summary of the meeting held 20<sup>th</sup> July 2015.  
  

**For Decision**  
(Pages 1 - 6)
4. **OUTSTANDING ACTIONS OF THE COMMITTEE**  
Members are asked to note the Committee's Outstanding Actions list.  
  

**For Information**  
(Pages 7 - 8)
5. **COMMITTEE WORK PROGRAMME**  
Members are ask to note the Committee's Work Programme.  
  

**For Information**  
(Pages 9 - 10)
6. **INTERNAL AUDIT UPDATE REPORT**  
Report of the Head of Internal Audit and Risk Management.  
  

**For Information**  
(Pages 11 - 20)
7. **CORPORATE RISK REGISTER UPDATE**  
Report of the Chamberlain  
  

**For Decision**  
(Pages 21 - 72)
8. **ANTI-FRAUD & INVESTIGATIONS UP-DATE REPORT**  
Report of the Chamberlain.  
  

**For Information**  
(Pages 73 - 82)
9. **CYBER SECURITY RISKS**  
Report of the Chamberlain  
  

**For Information**  
(Pages 83 - 106)

10. **HMIC INSPECTION UPDATE**  
Report of the Commissioner, City of London Police.

**For Information**  
(Pages 107 - 138)

11. **RE-APPOINTMENT OF AN EXTERNAL MEMBER**  
Report of the Town Clerk.

**For Decision**  
(Pages 139 - 140)

12. **QUESTIONS ON MATTERS RELATING TO THE WORK OF THE COMMITTEE**

**For Decision**

13. **ANY OTHER BUSINESS THAT THE CHAIRMAN CONSIDERS URGENT**  
The Chairman has agreed to the admission of an item of late business:

Risk Management – report of the Chamberlain (for information)

**For Information**  
(Pages 141 - 142)

14. **EXCLUSION OF THE PUBLIC**

**MOTION:** That under Section 100(A) of the Local Government Act 1972, the public be excluded from the meeting for the following items on the grounds that they involve the likely disclosure of exempt information as defined in Part I of the Schedule 12A of the Local Government Act.

**For Decision**

#### **Part 2 - Non-Public Agenda**

15. **NON-PUBLIC QUESTIONS ON MATTERS RELATING TO THE WORK OF THE COMMITTEE**
16. **ANY OTHER BUSINESS THAT THE CHAIRMAN CONSIDERS URGENT AND WHICH THE COMMITTEE AGREE SHOULD BE CONSIDERED WHILST THE PUBLIC ARE EXCLUDED**

This page is intentionally left blank

## AUDIT AND RISK MANAGEMENT COMMITTEE

Monday, 20 July 2015

Minutes of the meeting of the Audit and Risk Management Committee held at Guildhall, EC2 on Monday, 20 July 2015 at 1.45 pm

### Present

#### Members:

Alderman Nick Anstee (Chairman)  
Nigel Challis (Deputy Chairman)  
Alderman Charles Bowman  
Roger Chadwick (Ex-Officio Member)  
Henry Colthurst (Ex-Officio Member)  
Hilary Daniels (External Member)  
Revd Dr Martin Dudley  
Deputy Jamie Ingham Clark  
Oliver Lodge  
Alderman Timothy Hailes  
Kenneth Ludlam (External Member)  
Caroline Mawhood (External Member)  
Jeremy Mayhew (Ex-Officio Member)

#### Officers:

Paul Dudley	
Julie Mayer	Town Clerk's Department
Peter Kane	Chamberlain
Heather Bygrave	External Auditor, Deloitte
Chris Harris	

- 1. APOLOGIES**  
Apologies were received from Alderman Ian Luder and Graeme Smith.
- 2. MEMBERS' DECLARATIONS UNDER THE CODE OF CONDUCT IN RESPECT OF ITEMS ON THE AGENDA**  
There were no declarations.
- 3. MINUTES OF THE PREVIOUS MEETING**  
The Minutes of the Meeting held on 2 June 2015 were approved.
- 4. OUTSTANDING ACTIONS OF THE COMMITTEE**  
The Committee received its outstanding actions list and noted the following updates:

### **International Centre for Financial Regulation**

The Chamberlain advised that there had been a conviction and he would provide Members with further details shortly. This item could be removed from the action list.

### **Annual Governance Statement**

The amendments suggested by Members at the last meeting had been completed and approved (under delegated authority) and the document could now be formally signed off as part of the Statements of Accounts (at items 7 and 8 on this Agenda).

### **Corporate Risk Register (Governance)**

The Chamberlain advised that 3 further risks had been identified by the Chief Officers' Risk Management Group (CORMG) and they would be reported to the Committee in September. Members asked for the report to clarify a number of points raised in relation to the Committee's Terms of Reference. In respect of the Risk Challenge Sessions, Members suggested that once the current round of Chief Officer Risk Challenge Sessions was complete, the format might need to change, in order to keep it dynamic and relevant.

### **Peer Review**

As this had not been progressed across other authorities, officer would need to look at alternative benchmarking and report back to the Committee in due course. Members noted that, as a number of organisations were undertaking mock external reviews, this might be an option.

## **5. COMMITTEE WORK PROGRAMME**

The Committee received its latest work programme; updates since the last meeting were shown in italics.

## **6. PEER REVIEW**

This item was covered under item 4 (Outstanding Actions of the Committee).

## **7. AUDITED 2014/15 CITY FUND AND PENSION FUND FINANCIAL STATEMENTS TOGETHER WITH DELOITTE'S REPORT THEREON**

The Committee considered the 2014/15 City Fund and Pension Fund financial statements, together with Deloitte's report thereon. The Chairman was pleased at the high attendance (the previous week) at the Members' Briefings sessions on the Financial Statements. The Chamberlain advised that, subject to a satisfactory conclusion on a few areas still being reviewed by Deloitte, an unqualified opinion was expected and this position was confirmed by Deloitte. Members were advised that the Crossrail commitment of £200m from City Fund was now being shown as a note on the face of the balance sheet and that the payment was anticipated to be made by the end of March 2016.

Members were asked to note the following three areas still being reviewed:

- 1 Deloitte had challenged the City of London Corporation's treatment of proceeds from long leasehold disposals (e.g. in the case of the sale of 2 Fann Street). The City is currently treating the entire proceeds as capital receipts whereas Deloitte consider that there is an argument for part of the proceeds being treated as deferred income and released to revenue over the length of the lease (e.g. over 125 years). The issue revolves around interpretation as to whether the entire transaction can be treated as a finance lease (capital receipt) or whether the land element should be separated and treated as an operating lease (revenue). The Chamberlain advised that the outcome would inform how we treated future lease disposals.
2. The calculation of the provision for business rate appeals is complex and has required several iterations – the raw data set comprising 44,000 lines and a rateable value of £12.6 billion. Analyses have been prepared to try and determine trends over the past few years across a number of appeal categories, to identify potential duplicate claims on the Valuation Office list, to disregard settled appeals from the Valuation Office list, and to quantify refunds agreed in the old financial year but not paid until the new financial year. The latest estimate of the provision is with Deloitte for review.
3. Due to staff shortages in the Police Finance Team, Deloitte are awaiting information to support the treatment of a number of specific government grants. The backlog of requests is gradually being reduced and officers are confident that Deloitte will be able to conclude satisfactorily on the treatment of grant income.

Members were reminded that the accounts are required to be signed by 30th September 2015 and officers were confident that they would be ready ahead of the deadline. The process of delegation, as set out in the recommendations would be for the Town Clerk, in consultation with the Chairman and Deputy Chairman of the Audit and Risk Management Committee to recommend approval of any amendments to the Finance Committee. The Chamberlain would present these amendments in a revised income and expenditure account and balance sheet, with columns and notes setting out the movements between the original and revised versions.

Members were advised that, if the Chairman and Deputy Chairman deemed it necessary, the revisions would be shared with the entire Committee for comment, ahead of the financial statements being signed. The recommendation would then be considered by the Town Clerk, in consultation with the Chairman and Deputy Chairman of the Finance Committee.

**RESOLVED – THAT:**

1. The Town Clerk, in consultation with the Chairman and Deputy Chairman of the Audit and Risk Management Committee, approve any material changes to the financial statements required before the signing of the audit opinion by Deloitte; which is expected to be by the end of August or early September 2015.
2. Subject to the above, the accounts be recommended for approval to the Finance Committee.

8. **AUDITED 2014/15 BRIDGE HOUSE ESTATES AND SUNDRY TRUSTS FINANCIAL STATEMENTS TOGETHER WITH MOORE STEPHENS REPORT THEREON**

The Committee considered the 2014/15 Bridge House Estates, City's Cash Trust Funds and Sundry Trust Funds Annual Reports and Financial Statements together with Moore Stephens' report thereon. The Chamberlain advised that an unqualified audit opinion was expected and this position was confirmed by Moore Stephens. Moore Stephens advised that two risks, which had been highlighted in their Audit Plan when it was presented to the Committee in December, had been resolved satisfactorily. The Audit Review Panel had met and all Panel Members had approved the accounts.

Moore Stephens drew attention to the need to prepare in good time for the new Charity Accounting Regulations coming into effect for 2015/16, in particular that work on the 2014/15 comparators should start early.

**RESOLVED – THAT**, the Annual Reports and Financial Statements for Bridge House Estates, City's Cash Trust Funds and the Sundry Trust Funds for the year ended 31 March 2015 be recommended for approval to the Finance Committee.

9. **DECISIONS TAKEN UNDER DELEGATED AUTHORITY**

This had been covered under item 4 (Outstanding Actions) – Annual Governance Statement.

10. **QUESTIONS ON MATTERS RELATING TO THE WORK OF THE COMMITTEE**

There were no questions.

11. **ANY OTHER BUSINESS THAT THE CHAIRMAN CONSIDERS URGENT**

The Chairman thanked Deloitte for their services to the City of London Corporation, over a number of years, as this would be the last time they Audited the City Fund and Pension Fund Financial Statements.



**12. EXCLUSION OF THE PUBLIC**

**RESOLVED:** That under Section 100(A) of the Local Government Act 1972, the public be excluded from the meeting for the following items on the grounds that they involve the likely disclosure of exempt information as defined in Part I of the Schedule 12A of the Local Government Act.

<b>Items</b>	<b>Para no</b>
<b>12-13</b>	<b>-</b>

**13. NON-PUBLIC QUESTIONS ON MATTERS RELATING TO THE WORK OF THE COMMITTEE**

There were none.

**14. ANY OTHER BUSINESS THAT THE CHAIRMAN CONSIDERS URGENT AND WHICH THE COMMITTEE AGREE SHOULD BE CONSIDERED WHILST THE PUBLIC ARE EXCLUDED**

There were no items.

**The meeting ended at 3:00 pm**

-----  
Chairman

**Contact Officer: Julie Mayer  
tel. no.: 020 7332 1410  
julie.mayer@cityoflondon.gov.uk**

This page is intentionally left blank

## AUDIT AND RISK MANAGEMENT COMMITTEE - Outstanding Actions- September 2015 update

	<b>Item</b>	<b>Action</b>	<b>Officer responsible</b>	<b>Progress updates/target</b>
2	<b>Committee Satisfaction Survey</b> (added 4.11.14)	One of the Members offered to provide a pro-forma used within their place of business and Members agreed that input into future questions would be helpful.	Neil Davies	The next survey would take place next at the beginning of 2016 and the Committee would receive a further report on the method and style of the questionnaire in November 2015.
3	<b>Risk Challenge Sessions/deep dive reviews</b> (added 2.6.15)	It was suggested that the corporate risk deep dives be re-introduced, in order to complement the Chief Officer risk challenge sessions	Paul Dudley/ Julie Mayer	With effect from September, once the new risk register was in place.
4 Page 7	<b>Head of Internal Audit – Annual Opinion</b> (added 2.6.15)	<ol style="list-style-type: none"> <li>1. Members asked if future reports could provide a comparison with the previous years' performance and give greater visibility to improvements, - ie the regular inclusion of risk management reports on all Grand Committee agendas and the implementation of the Risk Challenge sessions.</li> <li>2. Peer Review - As this had not been progressed across other authorities, officer would need to look at alternative benchmarking and report back to the Committee in due course.</li> </ol>	Chris Harris/ Anna Simmonds/ Paul Dudley	<ol style="list-style-type: none"> <li>1. On-going.</li> <li>2. Members noted that, as a number of organisations were undertaking mock external reviews, this might be an option.</li> </ol>
6	<b>Corporate Risk Register Review</b> (added 2.6.15)	The Chamberlain advised that 3 further risks had been identified by the Chief Officers' Risk Management Group (CORMG) and they would be reported to the Committee in September. Members asked for the report to clarify a number of points raised in relation to the Committee's Terms of Reference.	Peter Kane	Next Corporate Risk Update - September 2015

AUDIT AND RISK MANAGEMENT COMMITTEE - Outstanding Actions- September 2015 update

	<b>Item</b>	<b>Action</b>	<b>Officer responsible</b>	<b>Progress updates/target</b>
7	<b>Cyber Fraud (added 2.6.15)</b>	Baker Tilly's Head of IT Audit will provide external advice on cyber fraud to inform the assessment of the level and types of risk facing the Corporation and the Committee would receive a presentation on the outcome of this work.	Chris Keesing Nirupa Gardener	Cyber Fraud Update on September's Agenda.

## ***Audit and Risk Management Work Programme 2015/16***

<b>Date</b>	<b>Items</b>
3 November	<ul style="list-style-type: none"> <li>• BDO – Annual Audit Plans for the City Fund and Pension Fund</li> <li>• Internal Audit Planning 2016/17</li> <li>• Audited 2014/15 City's Cash Financial Statements together with Moore Stephens report thereon</li> <li>• Deloitte's Annual Audit Letter on the City Fund and Pension Fund Financial Statements</li> <li>• Investigations Update Report</li> <li>• Committee Effectiveness Survey – method and style of questionnaire</li> </ul> <p><b><u>Risk Challenge Sessions:</u></b>  <b>Comptroller and City Solicitor</b>  <b><i>New Director of the Built Environment (to be confirmed)</i></b></p>
26 January 2016	<ul style="list-style-type: none"> <li>• Moore Stephens - annual audit plan for the Non Local Authority Funds</li> <li>• Internal Audit Progress Report</li> <li>• Internal audit recommendations follow-up report</li> <li>• Risk Management Update</li> </ul> <p><b><u>Risk Challenge Sessions:</u></b></p> <ul style="list-style-type: none"> <li>• <b>Boys' School</b></li> <li>• <b>Girls' School</b></li> <li>• <b>City of London Freemens' School</b></li> </ul>
8 <sup>th</sup> March 2016	<p>Investigations update report            Results of Committee Effectiveness Survey            Annual Governance Statement Methodology</p> <p><b><u>Risk Challenge Sessions:</u></b></p> <ul style="list-style-type: none"> <li>• <b>Culture, Heritage and Libraries</b></li> <li>• <b>Mansion House</b></li> </ul>
14 <sup>th</sup> June 2016	<p><b>Risk Challenge Session:</b></p> <ul style="list-style-type: none"> <li>• <b>Chamberlain</b></li> </ul>

This page is intentionally left blank

<b>Committee(s)</b>	<b>Dated:</b>
Audit and Risk Management Committee	17/09/2015
<b>Subject:</b> Internal Audit Update Report	<b>Public</b>
<b>Report of:</b> Head of Internal Audit and Risk Management	<b>For Information</b>

## Summary

This report provides an update on internal audit activity since the Committee last met. It also sets out the overall opinion of the Head of Internal Audit in relation to the adequacy and effectiveness of the control environment for those areas of internal audit work concluded since the last update report to Committee. The opinion is that the overall internal control environment is adequate and effective although some areas require strengthening.

The outcomes of the internal audit work finalised since the last Committee are summarised in Appendix 1. Seventeen assurance reviews have been finalised since the last report to the Committee. There were no Red reviews reported. Ten reviews resulted in Amber assurance opinions and seven in Green opinions. Both Amber and Green opinions represent adequate control environments.

As at 25 August 2015, 21% of the 2015-16 internal audit plan had been completed to draft report stage. Although this is fewer than expected, a further 41% of reviews are in progress and the internal audit plan is on target to be completed by 31 March 2016.

Audit follow up work demonstrates that the performance of the Corporation of London in implementing recommendations is generally effective with no Red recommendations outstanding which should have been implemented. 82% of the 57 Amber recommendations followed up had been implemented with a further 11% partially implemented. 7% of the recommendations had not yet been implemented but plans are in place to implement them and future progress will be reported to the Committee

## Recommendation(s)

Members are asked to note the update report.

## **Main Report**

### **Background**

1. This report sets out internal audit activity since the last report to Committee and the opinion of the Head of Internal Audit and Risk Management in relation to the adequacy and effectiveness of the control environment.

### **Current Position**

2. The outcomes of the internal audit work finalised since the last Committee have been reported to Members within the monthly briefings issued. Copies of these can be seen in **Appendix 1**. Seventeen assurance reviews have been finalised since the last report to the Committee. There were no Red reviews reported. Ten reviews resulted in Amber assurance opinions and seven in Green opinions. Both Amber and Green opinions represent adequate control environments.
3. In addition to Amber and Green reports, a further three reviews have been completed in respect of grant verification related work, along with the report on Cyber Security, which all had satisfactory outcomes.
4. No fundamental control failings that need to be brought to the attention of Members have been identified from the work performed to date in the 2015-16 plan

### **Internal Audit Section Performance and Delivery**

5. Performance levels against KPIs are generally good, although some improvement in the speed of delivery of audits is required and changes in working practices have been implemented to ensure the plan is delivered on time. Completion of the 2015-16 audit plan to draft report stage was 21% at 25 August 2015 which is below expected performance. However, a further 41% of the planned audits are in progress and there is sufficient time and resources to complete the remainder of the plan by 31 March 2016.
6. Details of performance levels against targets are set out below:



## Performance Indicators

Performance Measure	Target	Actual
1. Completion of the audit plan	100% of planned audits completed to draft report stage by end of plan review period (31 March 2016)	21%
2. Percentage (%) recommendations confirmed fully implemented at time of formal follow up	Red – 100% Amber – 80%	Red – n/a Amber – 82%*
3. Timely production of draft report	Average time taken to issue draft reports after end of fieldwork – target 28 days	27 days
4. Timely response to draft report	Average time taken to obtain a full management response after issue of draft report –target 28 days	24 days
5. Timely issue of final report	Average time taken to finalise the review after full response from management – target 7days	7 days
6. Customer satisfaction	Through key question on post audit surveys – target 90%	100%
7. Percentage (%) of audit section staff with relevant professional qualification	Target 75%	78%

\*Note – a further 11% were established to be partially implemented.

## Implementation of Audit Recommendations

- There are no RED recommendations outstanding beyond their due implementation dates. Follow up work since the last Committee has examined the implementation of 57 Amber recommendations. Of the 57 amber recommendations followed up we concluded that 47 (82%) had been fully implemented, 6 (11%) had been partially implemented and 4 (7%) had not yet been implemented. In the case of those that had not been implemented yet, plans are in place to resolve the issues and implementation will be reported to Members at a future meeting.

## Conclusion

- Internal Audit's opinion of the City's overall internal control environment is that it remains adequate and effective although some areas of the financial and operational framework do require strengthening by management as identified in Amber reports highlighted to the Committee in Members Briefings.

## Appendices

- Appendix 1 – Members briefings

### **Chris Harris**

Head of Internal Audit and Risk Management

T: 07800 513179

E: [chris.harris@cityoflondon.gov.uk](mailto:chris.harris@cityoflondon.gov.uk)

### Internal Audit Work 2015-16 (as at 25 August 2015)

This appendix compliments the summary outcome of final reports as presented in monthly Members briefings.

#### Progress against the plan – Summary

No of Reviews	Fieldwork	Draft Report	Final Report
74	11	10	5
	15%	14%	7%

Draft TOR = 19 (26%)

#### Progress against the plan - Detail

Department	Main Audit Review	Status*	Assurance**	Recommendations Made**				Recommendations Agreed**					
				R	A	G	Total	R	A	G	Total		
Corporate	Business Continuity & Disaster Recovery	<i>Draft TOR</i>											
Corporate	Supporting Businesses	<i>Draft TOR</i>											
Corporate	Information Governance and Security (Cyber Security Committee Report)	FINAL	n/a	n/a				n/a					
Corporate	Health & Safety	Fieldwork											
Corporate	Learning & Development												
Corporate	Vetting of Staff												
Corporate	COSO - Entity Wide Control Environment												
Corporate	Procurement												
Corporate	Petty Cash	Fieldwork											
Corporate	Cash Income Collection and Banking	Fieldwork											
Corporate	Expenses	Fieldwork											
Corporate	Pre Contract Appraisal	<i>Draft TOR</i>											
Corporate	Liquidations	Fieldwork											
Corporate	Follow Ups												
Corporate	Physical Access Security to Guildhall												
Chamberlain	Main Accounting System - GL / AR / AP	<i>Draft TOR</i>											
Chamberlain	Investments - Corporate Responsibility												
Chamberlain	Council Tax												
Chamberlain	Business Rates												
Chamberlain	Governance and Oversight of Service Based Reviews												
Information Systems	ITIL Compliance	Fieldwork											
Information Systems	Remote Access	<i>Draft TOR</i>											
Information Systems	Database Patching & Change Control Procedures	<i>Draft TOR</i>											
Information Systems	Back Up Strategy and Procedures	Fieldwork											

Department	Main Audit Review	Status*	Assurance**	Recommendations Made**				Recommendations Agreed**				
				R	A	G	Total	R	A	G	Total	
Information Systems	Firewalls	<i>Draft TOR</i>										
Information Systems	Asset Register	<i>Draft TOR</i>										
Information Systems	WAN (MLPS)	<i>Draft TOR</i>										
Information Systems	GJR Server Rooms											
Information Systems	People's Network (Culture, Heritage & Libraries)											
Information Systems (Outsourced)	WIFI Strategy											
Information Systems (Outsourced)	Cloud Security											
Information Systems (Outsourced)	Oracle 12 Licenses											
Information Systems (Outsourced)	Oracle Post Implementation Review											
Open Spaces	Hampstead Heath	<i>Draft</i>										
Open Spaces	Cemeteries & Crematoriums	<i>Draft TOR</i>										
Open Spaces	Chingford Golf Course											
Markets and Consumer Protection	Licensing	<i>Draft TOR</i>										
Markets and Consumer Protection	Port Health Income	<i>Draft</i>										
Markets and Consumer Protection	Penalty Charge Notices	FINAL	Amber	0	3	3	6	0	3	3	6	
Community & Children Services	Departmental Review											
Community & Children Services	Sir John Cass Schools Financial Value Sign Off	<i>Draft</i>										
Community & Children Services	Sir John Cass School Private Fund Account	Fieldwork										
Community & Children Services	Community Capacity and Disabled Facilities Grant Verification	FINAL	n/a	n/a				n/a				
City Surveyors	Property Purchases, Sales & Investments	<i>Draft TOR</i>										
City Surveyors	Rents, Letting and Vacancies	<i>Draft TOR</i>										
Built Environment	Recoverable Works	<i>Draft TOR</i>										
Police	Expenses (inc. travel expenses )											
Police	Business Travel Scheme											

Department	Main Audit Review	Status*	Assurance**	Recommendations Made**				Recommendations Agreed**				
				R	A	G	Total	R	A	G	Total	
Police	Police Officer Allowances & Ad Hoc Payments											
Police	Police Supplies & Services and 3rd Party Payments	Fieldwork										
Police	Action Awareness Team											
Police	Governance and oversight of outsourcing (IT)											
Police	Interim Follow Up of Disaster Recovery and PBX Resilience	Draft										
Police	Invoices on Hold	Draft										
Police	Interpreters Fees	Draft										
Police	Gifts and Hospitality	Fieldwork										
Police	European Commission Grant Verification	FINAL	n/a				n/a					n/a
CLFS	Institutional Review	<i>Draft TOR</i>										
CLS	Institutional Review	<i>Draft TOR</i>										
CLSG	Institutional Review	<i>Draft TOR</i>										
CLSG	ICT Strategy	Draft										
Guildhall School	Annual Enrolment											
Guildhall School	Milton Court	<i>Draft TOR</i>										
Guildhall School	Procurement of Goods and Services	Draft										
Guildhall School	Satellite Operations											
Barbican	Box Office											
Barbican	Barbican - International Enterprise	Fieldwork										
Barbican	Barbican - Bars (Contract Management and New Arrangements)											
Barbican	Membership Scheme											
Barbican	Budget Setting and Financial Management	<i>Draft TOR</i>										
Barbican	Cost Estimates and Cost Plan	FINAL	Green	0	1	1	2	0	1	1	2	
Barbican	Systems Controls											
Culture Libraries and Heritage	Monument Cash Collection	Draft										
Mansion House	Annual Plate Review	Draft										

\*Status definitions – Fieldwork = Formal TOR issued, Draft = Formal draft report issued, Final = Review complete and final report issued.

\*\* Only completed once final report has been issued.

### Progress against the plan – Additions and Deletions

The changes below have currently been accommodated from the original contingency budget available (48 days):

Additions			Deletions		
Title of Review	Reason for Addition	No of Days	Title of Review	Reason for Addition	No of Days
Sir John Cass Primary School – Schools Financial Value Statement Sign Off	Work performed to provide assurance to the Chamberlain regarding the sign off of the statement.	-6	Open Spaces – Donations and Sponsorship Income	As a result of discussions with Director agreed that not high risk and would be more appropriate to review during 2016/17 and focus on other types of funding.	+15
Sir John Cass Primary School – Private Fund Account Sign Off	Request for internal audit to review and sign off accounts.	-4.5			
Monument Cash Collection	Work performed to ensure that income collection and ticket sales are well controlled following information provided by a member of the public.	-6			
Interim Follow Up of Disaster Recovery and PBX Resilience	Police management have requested that interim follow up review is performed of these two reviews that received 'red' assurance opinions.	-6			
Police Interpreters Fees	Carry forward from 2014-15 internal audit plan	-5			
Police Gifts and Hospitality	Request from Performance and Resources Sub Committee	-6			
Community Capacity and Disabled Facilities Grant	Request from finance staff to complete the verification of two grant returns.	-3			
European Commission Grant	Request from finance staff to complete the verification of the grant return.	-5			
Mansion House	Annual Plate Review	-2			
Open Spaces	Additional budget required to complete the Hampstead Heath review due to changes in approach. Furthermore, this was the first review done through joint working.	-2.5			
	Total	-46		Total	+15

## Performance Indicators

Performance Measure	Target	Actual
1. Completion of the audit plan	100% of planned audits completed to draft report stage by end of plan review period (31 March 2016)	17%
2. Percentage (%) recommendations confirmed fully implemented at time of formal follow up	Overall – 75% Red – 100% Amber – 80%	72% Red – n/a Amber – 72%*
3. Timely production of draft report	Average time taken to issue draft reports within 28 days of end of fieldwork i.e. exit meeting date.	27 days
4. Timely response to draft report	Average time taken to obtain a full management response within 28 days of the draft report being issued	24 days
5. Timely issue of final report	Average time taken to finalise the review within 7 working days on full response from management	7 days
6. Customer satisfaction	Through key question on post audit surveys – target 90%	100%
7. Percentage (%) of audit section staff with relevant professional qualification	Target 75%	78%

Page 19

\*Note – a further 20% were established to be partially implemented.

This page is intentionally left blank



<b>Committee:</b>	<b>Date:</b>
Audit and Risk Management Committee	17 September 2015
<b>Subject:</b> Corporate Risk Register Update	<b>Public</b>
<b>Report of:</b> Chamberlain	<b>For Decision</b>

## Summary

This report presents the Audit and Risk Management Committee with the outcome of the corporate risk identification review and an update on “deep dive reviews” of corporate risks and provision of detailed risk information referred to the Chief Officer’s Risk Management Group (CORMG) by the Committee on 2 June 2015.

Summit Group met on 13 July 2015 and confirmed the recommendations of CORMG in relation to the changes to the corporate risk register (now making a total of nine corporate risks) and also suggested that two new corporate risks be developed on Road Safety and Air Quality.

## Recommendations

### Members are asked to:

- Note the outcome of corporate risk identification review by the CORMG on 25 June 2015 and subsequent agreement of the Summit Group to the changes to the corporate risk register.
- Note that two new risks (Road Safety and Air Quality) are being prepared and if approved by the Summit Group in September 2015, will be included in the risk update report to the Committee in November 2015.
- Agree to reinstate “deep dive “ corporate risk reviews as outlined in paragraph 3.4 below and to identify which corporate risk the Committee wishes to review in January 2016.

## Main Report

### 1.0 Background

- 1.1 Summit Group, at their meeting on the 18 May 2015, received a report on the outcome of the review of the corporate risk register undertaken by the CORMG. The report recommended that three risks (see para 1.2 below) be removed from

the corporate risk register along with other changes, thereby reducing the number of risks on the corporate risk register from 10 to seven risks. Summit Group approved the recommendations and noted that CORMG would be undertaking an exercise to identify and assess any new risks that should be recommended to the Summit Group for inclusion on to the corporate risk register at their meeting on 25 June 2015. The results of this exercise are reported below (paras 2.5 and 2.6).

- 1.2 The Audit and Risk Management Committee on 2 June 2015 received the risk update report which included details of changes to the corporate risk register. The Committee recommended that CORMG “consider a number of issues raised on the following corporate risks – CR08 reputation, CR14 funding reduction and CR 18 workforce (staff shortage and capacity)”. They also identified a number of other matters for CORMG to consider and these are responded to in para 3.0 below.
- 2.0 **Corporate risk register**
- 2.1 The Audit and Risk Management Committee requested CORMG to review their recommendation for de-escalating the following corporate risks: CR14 funding reduction and CR18 workforce (staff shortage and capacity) and the removal from the register of CR08 reputation risk.
- 2.2 CORMG reviewed these risks, at their meeting on 25 June 2015, and agreed that Summit Group be asked to confirm:
  - a) **CR08 reputation.** This risk should be **removed** from the corporate risk register as reputational damage is regarded as an impact of another event occurring rather than a risk in itself. In future the Director of Public Relations would arrange for a PR officer to be responsible for reviewing the corporate risks, ensuring that reputational impacts of a risk occurring were appropriately articulated in risk descriptions and scoring.
  - b) **CR 14 Funding Reduction.** This risk should be **reinstated** as a corporate risk at least until the outcome of the Budget and the Spending Review was known.
  - c) **CR 18 workforce (staff shortage and capacity).** This risk should be **de-escalated** to departmental level. Whilst there were important areas within the Corporation that had difficulty in recruiting and retaining staff (such as IT), the primary focus should be on departmental mitigations. In future, however, this risk would be regarded as “top red risk” and reported to Summit Group and the Audit and Risk Management Committee in the Risk update reports. (See addendum to appendix 2)
- 2.3 Summit Group, at their meeting on 13 July 2015, confirmed the above recommendations. Table 1 below shows the corporate risks taking account of the removal of CR08 and CR18 and reinstating CR14, in current score order.

<b>Risk no</b>	<b>Risk title</b>	<b>Risk rating</b>	<b>Risk score</b>
CR11	Hampstead Heath Ponds	Red	16
CR 19	IT Service Provision - Police and Corporation IT Service	Red	16
CR09	Health and Safety Risk	Amber	12
CR01	Resilience Risk	Amber	8
CR02	Supporting the Business City	Amber	8
CR10	Adverse Political Developments	Amber	8
CR17	Safeguarding	Amber	8
CR14	Funding Reduction	Amber	6
CR16	Information Security	Amber	4

2.4 With the exception of CR19 none of the eight corporate risks in table 1 above have changed in risk score since the last report to the Audit and Risk Management Committee on 2 June 2015. Risk no CR10 has, however a revised risk description.

#### **Proposed new corporate risks**

2.5 CORMG, at their meeting on 25 June 2015, reviewed the 12 top red departmental risk register and considered that none of these warranted escalation to the corporate risk register. Since that review – the City Surveyor’s red risk - Failure of the Property Management System (Manhattan) has been rescored to amber following progress in mitigating this risk. Recently one new red risk has been added to this risk register, now making a total of 12 top red departmental risks. These risks are shown in appendix 2. Both the top red departmental risks and corporate risks will be reviewed at the next meeting of CORMG which takes place on 30 September 2015.

2.6 CORMG considered the following risks for inclusion in the corporate risk register and made recommendations on each risk to the Summit Group on 13 July 2015:

- a) **Road Safety-** given the recent tragic cycling accident at Bank Station and wider concerns about road safety in the City, CORMG recommended to the Summit Group, that road safety risk should be escalated to the corporate risk register. The Summit Group considered that a new road safety risk should be produced, by the Director of Built Environment, encompassing the reputational impacts on the City Corporation and re-present it at its meeting in September 2015. If approved by the Summit Group it will be reported to the Audit and Risk Management Committee in November 2015.
- b) **MCP-EH 001 Air Quality.** There was little action that the City Corporation could take to mitigate the financial effects of this risk. The primary focus should therefore be on the health aspects - CORMG required further information on the mitigations and position of the GLA and other authorities. Pending this further information, Summit Group agreed that

this risk should not be escalated on to the corporate risk register It will be presented to Summit Group at its meeting in September 2015 and if approved reported to the Audit and Risk Management Committee in November 2015.

c) **CHB005 IT Service Provision - Police and Corporation IT Service.**

The whole Police IT infrastructure and parts of the Corporation are in need of further investment as there is a risk of critical failure of Police IT systems and for the Corporation, poor performance of IT systems. Summit Group agreed that this risk should be escalated on to the corporate risk register.

2.7 Summit Group agreed, that with immediate effect, the IT Service provision risk should be added to the corporate risk register, making a total on 9 corporate risks (See appendix 1). Two new corporate risks are in preparation (Road Safety and Air Quality) and will be brought to the Summit Group in September 2015. If approved they will be reported to the Audit and Risk Management Committee in November 2015.

**3.0 Update to the Audit and Risk Management Committee recommendations – 2 June 2015.**

3.1 In addition to requesting a review of the three risks to be removed from the corporate risk register, the Committee requested further information on corporate and other risks and requested CORMG consider re-introducing “deep dive” reviews of individual risks at formal Committee meetings. An update is provided below on each of these points.

**Detailed risk information**

3.2 The Committee requested details of the risks considered but not recommended for inclusion on the revised corporate risk register to be submitted at their September 2015 meeting. CORMG considered in particular the existing top red departmental risks. Members also requested to receive mitigation information in regard to these and corporate risks. Appendix 1 and 2 contains corporate and top red department risk registers showing the mitigations for each risk.

**“Deep Dive” Corporate risk reviews**

3.3 The Committee asked CORMG to consider the possibility of re-introducing the “deep dive” reviews of corporate risks within the formal meetings. This would be in addition to the departmental informal risk challenges which take place prior to each Committee meeting. CORMG recognised the potential value of these reviews. It is suggested that one corporate risk reviewed at each meeting (except for the July meeting). The relevant risk owner would be requested to prepare a report on the risk, mitigations and progress on its overall management and present the report at the relevant Committee meeting. If the Committee agree then this new arrangement would take effect from January 2016 meeting.

## **4.0 Conclusion**

- 4.1 The Corporate risk register continues to be actively reviewed and updated by risk owners in line with the requirements stipulated by the Risk Management Strategy. CORMG provides additional assurance to the Summit Group, COG and the Audit and Risk Management Committee that corporate risks are appropriate and being actively managed.

### **Appendices:**

- **APPENDIX 1** Corporate Risk Register (Detailed report)
- **APPENDIX 2** Top Red departmental risk register (Detailed report)

**Contact:**

*Paul.Dudley | Paul.Dudley@cityoflondon.gov.uk | 0207332 1297*

This page is intentionally left blank

Corporate risks as at 21 August 2015

Code	Title	Current Rating	Page no
CR11	Hampstead Heath Ponds - overtopping leading to dam failure	16	1
CR19	IT Service Provision	16	5
CR09	Health and Safety Risk	12	8
CR01	Resilience Risk	8	9
CR02	Supporting the Business City	8	10
CR10	Adverse Political Developments	8	11
CR17	Safeguarding	8	12
CR14	Funding Reduction	6	15
CR16	Information Security	2	18

This page is intentionally left blank



# Corporate risk register

Generated on: 21 August 2015

Appendix 1



Rows are sorted by Risk Score

## Code & Title: CR Corporate Risk Register 9

Risk No. & Title	Risk Description (Cause, Event, Impact)	Risk Owner	Current Risk Rating & Score	Risk Update	Target Risk Rating & Score	Target Date	Risk Trend
CR11 Hampstead Heath Ponds – overtopping leading to dam failure	<p><b>Cause:</b> The earth dams on Hampstead Heath are vulnerable to erosion caused by overtopping</p> <p><b>Event:</b> Severe rainfall event which causes erosion which results in breach, leading to failure of one or more dams</p> <p><b>Impact:</b> Loss of life within the downstream community and disruption to property and infrastructure – including Kings Cross station and the Royal Free Hospital. A major emergency response would need to be initiated by Camden Council and the police at a time when they are likely to already be dealing with significant surface water flooding. Damage to downstream buildings and infrastructure would result in</p>	Sue Ireland	<p>Likelihood</p> <p>Impact</p>	<p>The "Ponds Project" has been initiated to address the vulnerability of the dams to overtopping and the associated erosion. As this project is the ultimate mitigation of this risk and all other feasible mitigations are already in place, the issues reported related principally to the successful and timely completion of the Ponds Project.</p> <p><b>Potential for land ownership issues to cause delays</b>– The various adjoining landowners have been engaged with and there is no concern currently that this will impact on project progression.</p>	<p>Likelihood</p> <p>Impact</p>	31-Oct-2016	↔

Page 29

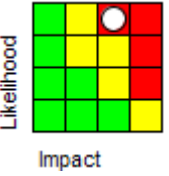
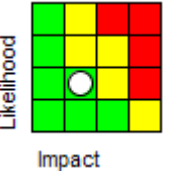
	<p>significant re-build costs. The City's reputation would be damaged. An inquiry and legal action could be launched against the City.</p> <p>The Ponds Project has been initiated to mitigate this risk as the current interim mitigations of telemetry, weather monitoring, an on-site emergency action plan do not address the issue of the dam's vulnerability to overtopping</p>			<p><b>Potential for protest</b> – Officers have engaged with Met Police, Camden and specialist contractors to ensure that we are in a position to respond to any protest which occurs. A "Gold Strategic Intent" document has been drafted. This sets out the principles of accommodating protest which is safe, peaceful and non-disruptive.</p> <p><b>Health &amp; Safety</b> – The Heath is a public open space and therefore the interaction between people, dogs and construction plant must be managed. All construction vehicles will be escorted and move at walking pace.</p> <p><b>Cost increases</b> – The budget is managed by the Project Board. A separate risk contingency has been established.</p> <p><b>Further challenge</b> – Although much reduced following the JR and planning decision, some local groups are continuing to lobby government to</p>			
--	---	--	--	---	--	--	--

				prevent the project.			
--	--	--	--	----------------------	--	--	--

Action Code & Title	Action Description	Action Owner	Due Date	Action Update
CR11 a Project Director to review budget monthly with Project Board – specific consideration of use of risk contingency	Regular monitoring of budget and risk provisions	Paul Monaghan	31-Mar-2016	Project Director continues to monitor the budget closely with the project officer.
CR11 b Agreement of methods of working with utilities	Agreement of methods of working with utilities	Paul Monaghan	31-Aug-2015	Engineers and Contractor have been meeting regularly with utilities
CR11 c Site supervision by DBE and OS to ensure appropriate H&S procedures	Regular review of H&S and working practices – in particular movement of vehicles	Paul Monaghan	31-Mar-2016	Weekly meetings to review practices being undertaken
CR11 d Liaison Officer to engage proactively through site notices, media, electronic	Liaison officer role defined by planning conditions in respect of CWG, but will undertake broader community engagement role as previously	Paul Monaghan	31-Mar-2016	CWG continues to meet regularly alongside a programme of walks

communications, PPSG and CWG				
CR11 e New on-site plan to be agreed by Core Group and Project Board	A revised on-site plan is required for the construction period.	Paul Monaghan	31-Aug-2015	New plan was agreed by the core group subject to approval by the panel engineer. Project officer to follow up with Atkins on this approval
CR11 f Daily ecological monitoring by BAM and Heath staff to check for nesting birds	As per planning consent and conditions	Paul Monaghan	31-Oct-2016	Daily monitoring will take place until the conclusion of the works.
CR11 g Weekly site meetings to secure clear communication between OS, DBE and BAM	To secure clear understand of impact on the Heath, resolution of any issues, discussion of complaints	Paul Monaghan	31-Oct-2016	Meeting continue to progress well
CR11 h Resolution of issues with adjoining land owners	There are 4 different adjoining landowners who the City is engaging with. The land ownership will be resolved according to the specifics of each case – via transfer, access agreements or registration as co-undertakers with the EA	Paul Monaghan	31-Aug-2015	Negotiations ongoing

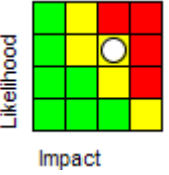
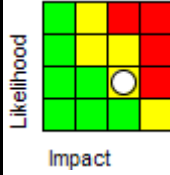
CR11 i Approval of designs for Highgate 1	The design approved for Highgate 1 impacts on another landowner. Discussions as to an acceptable alternative have been progressing. Any change will require planning permission.	Paul Monaghan	31-Aug-2015	Further discussions with landowner required
---	--	---------------	-------------	---

Risk No. & Title	Risk Description (Cause, Event, Impact)	Risk Owner	Current Risk Rating & Score	Risk Update	Target Risk Rating & Score	Target Date	Risk Trend
CR19 IT Service Provision Page 33	<p><b>Cause:</b> The whole Police IT Estate and parts of the Corporation are in need of further investment.</p> <p><b>Event:</b> For the Corporation, poor performance of IT Service and for the Police critical failure of the Police IT Service.</p> <p><b>Effect:</b> Loss of communications or operational effectiveness (including service performance, reliability and weakening DR capabilities). reputational damage. Possible failure of critical Corporation and Policing activities.</p>	Graham Bell	 16	The Agilisys Service take on from Dec 2014 has 8 mandatory projects design to improve the Police IT Infrastructure. A Joint Network Refresh has also been initiated to update and renew the Police network both between and within Buildings. Taken together these two projects will greatly improve the IT service and reduce the risk to an acceptable level.	 4	31-Dec-2015	↔

Action Code & Title	Action Description	Action Owner	Due Date	Action Update
CR19a COLP Agilisys managed	Agilisys managed services contract will bring additional resource and a resilient data centre solution to the	Graham Bell	31-Dec-2015	ACTION COMPLETED. The Agilisys service take-on commenced in December 2014. With the exception of the major storage, failure in late June the service take-on has been smooth,

services contract.	Police IT estate.			<p>improved service reliability and there are significantly improved resources, process and procedure in place.</p> <p>The 8 mandatory projects are progressing well and to plan and Agilisys are considering further actions which may mitigate the risks in the short-term pending completion of the projects.</p>
CR19b JOINT Network refresh programme.	Joint network refresh programme to resolve issues around network resilience and ensure we have diverse routes for network traffic, avoiding single points of failure.	Graham Bell	31-Dec-2015	<p>A Gateway 3 has been approved by Force Change Board and Capital Programme Board within CoLP, and will be presented to Project Sub Committee for approval. GYE is now operating with a new local area network and the Police Telephony system has completed an upgrade to improve resiliency, there is provision within the Gateway 3 Paper to return for urgent items which need to be resolved quickly while the longer term solution is implemented for other Police Buildings</p> <p>For the Corporation the existing LAN is supported by an IBM Support contract and is operating satisfactorily, however equipment is end of life there is a risk of failure and must be replaced under the JNRP.</p>
CR19c JOINT End User Device Renewal	Investment in any retained IT infrastructure to ensure that this meets the same standards of resilience and continuity as delivered by the IaaS infrastructure.	Graham Bell	31-Mar-2016	<p>For the Police this work has already been completed and the end user device estate has been renewed.</p> <p>For the Corporation a Gateway 2 Report has been prepared to replace the 60% of devices now more than 4 years old, as well as making improvements to supporting infrastructure and systems. If approved this should be completed by Mar 2016</p>
CR19d CoLP Investment in any retained IT infrastructure	Investment in any retained IT infrastructure to ensure that this meets the same standards of resilience and continuity as delivered by the IaaS infrastructure	Graham Bell	31-Dec-2015	<p>A gateway 1 / 2; has been approved for the refreshment of the retained IL4 infrastructure for CoLP.</p>

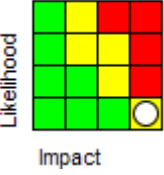
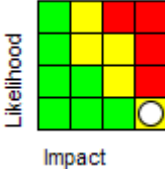
CR19e CoLP Progress review scheduled for May 2015.	Investment in any retained IT infrastructure to ensure that this meets the same standards of resilience and continuity as delivered by the IaaS infrastructure.	Graham Bell	31-May-2015	ACTION COMPLETED. Review has been completed and although projects are progressing to plan. We are working with Agilisys to seek early mitigation of some areas of risk.
CR19f JOINT Migration of servers to dual data centre.	Staff available out of hours to cover any issues.	Graham Bell	31-May-2015	ACTION COMPLETED. IAAS Project – Migration of servers to dual data centre.
CR19g CoLP Staff availability.	Staff available out of hours to cover any issues.	Graham Bell	12-Mar-2015	ACTION COMPLETED. Agilisys now have a resourced team in place to support the Police and ensure support is available 24 / 7.
CR19h DR Capabilities	There are DR capabilities which mean any critical failures can be recovered from, although should be noted that limitations within these capabilities might mean that systems may not be restored within recovery time objectives.		12-Mar-2015	ACTION COMPLETED. Improved procedure and processes are now in place and there is capability available to recovery from problems as quickly as the current infrastructure allows.
CR19i CoLP Recovery activity documentation.	Documentation in place to support recovery activity.	Graham Bell	12-Mar-2015	ACTION COMPLETED. Improved procedure and processes are now in place and there is capability available to recovery from problems as quickly as the current infrastructure allows. Additionally, as new IaaS infrastructure is deployed procedures will be enhanced.
CR19j CoLP Transition plan.	Transition plan in place to deliver sustainable and resilient DR capabilities.	Graham Bell	12-Mar-2015	ACTION COMPLETED. The 8 Mandatory Agilisys projects are planned, resourced and managed

Risk No. & Title	Risk Description (Cause, Event, Impact)	Risk Owner	Current Risk Rating & Score	Risk Update	Target Risk Rating & Score	Target Date	Risk Trend
CR09 Health and Safety Risk	<p><b>Cause</b> – Safety is treated as a low priority by the organisation, lack of training of staff and managers, management complacency, poor supervision and management</p> <p><b>Event</b> – Statutory regulations and internal procedures relating to Health and Safety breached and/or not complied with.</p> <p><b>Effect</b> – Possible enforcement action/ fine/prosecution by HSE, Employees/visitors/contractors may be harmed/injured, Possible civil insurance claim, Costs to the Corporation, Adverse publicity /damage to reputation, Rectification costs</p>	Chrissie Morgan	 12	<p>The risk was reviewed by the SMT on 20/08/15, no change to the assessment at this time</p> <p>External accreditation of the CoL Health and Safety Management System is due to take place in November</p> <p>The Top X risk assessment approach is being repackage to bring the process in line with the Covalent risk management software</p>	 8	31-Mar-2016	↔

Page 36

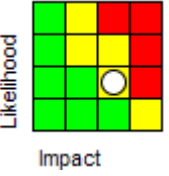
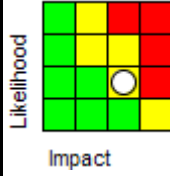
Action Code & Title	Action Description	Action Owner	Due Date	Action Update
CR09A External Verification	External verification of the CoL's safety management system	Oliver Sanandres	30-Nov-2015	Action added 240615, currently selecting appropriate review organisation
CR09B Compliance Audits	Rolling programme of departmental compliance audits conducted by the Corporate Health and Safety Unit	Oliver Sanandres	31-Mar-2016	Work for this financial year started April 1 2015, 2 audits currently completed, programme for the rest of the year has been set and is on target



Risk No. & Title	Risk Description (Cause, Event, Impact)	Risk Owner	Current Risk Rating & Score	Risk Update	Target Risk Rating & Score	Target Date	Risk Trend
CR01 Resilience Risk	<p><b>Cause</b> – Lack of appropriate planning, leadership and coordination</p> <p><b>Event</b> – Emergency situation related to terrorism or other serious event/major incident is not managed effectively</p> <p><b>Effect</b> – Major disruption to City business, failure to support the community, assist in business recovery</p>	John Barradell	 <p>8</p>	This risk was review by the SMT and the assessment score is rated as unchanged Exercise Allovus was conducted on June 11 successfully. The exercise included the emergency services. The findings from the exercise will be reported to the Summit Group on July 13	 <p>8</p>	31-Mar-2016	↔

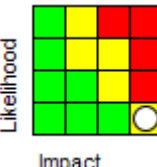
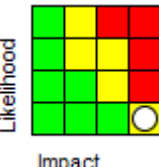
Page 37

Action Code & Title	Action Description	Action Owner	Due Date	Action Update
CR01A Emergency Exercise	Full exercise (Allovus) to test the emergency and business continuity plans across the organisation. The exercise will involve the emergency services	Gary Locker	11-Jun-2015	The exercise was completed as planned
CR01B Exercise Allovus – review report to Senior Management	Prepare and complete a review report for the Summit Group, actions leading from Exercise Allovus	Gary Locker	31-Oct-2015	Report was originally planned to be complete in July 2015, but further work was required and the report will now be submitted to Senior Management by the end of October 2015

Risk No. & Title	Risk Description (Cause, Event, Impact)	Risk Owner	Current Risk Rating & Score	Risk Update	Target Risk Rating & Score	Target Date	Risk Trend
CR02 Supporting the Business City	<p><b>Cause</b> – The City Corporation’s actions to promote and support the competitiveness of the business City do not succeed.</p> <p><b>Event</b> – The City’s position as the world leader in international financial services is adversely affected</p> <p><b>Effect</b> – The City loses its ability to attract and retain high value global business activity, both as a physical location and in mediating financial and trade flows; the City Corporation’s business remit is damaged and its perceived relevance is diminished.</p>	John Barradell	 8	Following review the risk assessment/scoring is unchanged The Corporation and the International Regulatory Strategy Group ensure we engage on the key regulatory issues that affect the financial and professional services industry, informing our engagement with policy makers, regulators and the media. ED office is engaged in a programme of work to support, defend and enhance the business city, in accordance with ED Business Plan.	 8	31-Mar-2016	↔

Action Code & Title	Action Description	Action Owner	Due Date	Action Update
CR02A Special Representative of the City to the EU	Appointment of former Foreign Office Minister, Jeremy Browne, to new position to enhance our engagement with EU policy makers.	Giles French	01-Sep-2015	Appointment Commences on 1 September 2015 – 3 year appointment

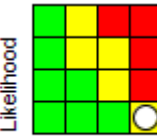
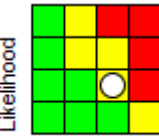
CR02B Restructure of the team working on financial and professional services	City, EU and International Affairs teams have been restructured into City Competitiveness and Regulatory Affairs teams to remove geographical boundaries and provide greater policy focus to work. Job descriptions have been reviewed for same purpose.	Giles French	01-Sep-2015	New structure and roles go live on 1 September 2015
---	--	--------------	-------------	---

Risk No. & Title	Risk Description (Cause, Event, Impact)	Risk Owner	Current Risk Rating & Score	Risk Update	Target Risk Rating & Score	Target Date	Risk Trend
CR10 Adverse Political Developments Page 39	<p><b>Cause:</b> Financial services issues that make the City Corporation vulnerable to political criticism; local government devolution proposals that call into question the justification for the separate administration of the Square Mile.</p> <p><b>Event:</b> Functions of City Corporation and boundaries of the City adversely affected.</p> <p><b>Impact:</b> The future of the City of London Corporation as an independent body could be undermined.</p>	Paul Double	 8	<p>There has been close engagement with those responsible for developing proposals to enable the devolution of responsibilities while safeguarding the City. Constant attention is given to the form of legislation affecting the City. Continued promotion of the good work of the City Corporation among opinion-formers particularly in Parliament and Central Government so that the City Corporation is seen to remain relevant and "doing a good job" for</p>	 8		↔

				London and the nation .			
--	--	--	--	-------------------------	--	--	--

Action Code & Title	Action Description	Action Owner	Due Date	Action Update
CR10a Government and stakeholder engagement	Monitoring of Government legislation and proposed regulatory changes. Provision of information to Parliament and Government on issues of importance to the City. Engagement with key opinion informers in Parliament and elsewhere. Programme of work to monitor and respond to issues affecting the reputation of the City Corporation.	Paul Double	31-Mar-2016	Relevant Bills in the Government's legislative programme have been identified and City Corporation departments alerted to issues of potential significance. Briefing has been provided for Parliamentary debates on air quality, immigration, the creative industry, trade and investment, Fintech and broadband. There has been continuing engagement on devolution in London and liaison with London Councils and Central London Forward on the application of devolution to the London boroughs and the City, either directly from central Government or the Mayor.

Page 40

Risk No. & Title	Risk Description (Cause, Event, Impact)	Risk Owner	Current Risk Rating & Score	Risk Update	Target Risk Rating & Score	Target Date	Risk Trend
CR17 Safeguarding	<b>Cause:</b> Not providing appropriate training to staff, not providing effective management and supervision, poor case management <b>Event:</b> Failure to deliver actions under the City of London' safeguarding policy. Social workers and other staff not taking appropriate action if notified of a safeguarding issue	Ade Adetosoye	 Likelihood Impact	Work is ongoing to raise awareness of safeguarding, through e-learning, briefing sessions and working with partners. Good progress has been made on implementing the actions to mitigate this risk.	 Likelihood Impact	31-Mar-2016	↔

	<b>Effect:</b> Physical or mental harm suffered by a child or adult at risk, damage to the City of London's reputation, possible legal action, investigation by CQC and or Ofsted						
--	---	--	--	--	--	--	--

Action Code & Title	Action Description	Action Owner	Due Date	Action Update
CR17b Work with HR to develop training and programmes to support staff	Develop safeguarding e-learning modules and enable staff to access advice and assistance	Chris Pelham	30-Sep-2015	The majority of staff have undertaken the e-learning modules. Outstanding training will be completed by end of August
CR17c Safeguarding Awareness Sessions for DCCS Staff	3 raising awareness sessions will be delivered to Community and Children's Services staff. These sessions will cover updated Child Sexual Exploitation and Children Missing from home, Education and or Care protocols and referral process which have been updated and circulated to all professionals. A Multi Agency Sexual Exploitation group is now fully functioning.	Chris Pelham	31-Jul-2015	Completed - All sessions have now been delivered to staff.

CR17d Raising awareness of Private Fostering, role of Local Authority Designated Officer (LADO)	A Multi Agency Briefing Event will be held with over 60 partners attending to launch the new referral process, to highlight the role of the Local Authority Designated Officer and raise awareness Private Fostering and the City of London Thresholds document.	Chris Pelham	30-Sep-2015	Completed – the briefing session took place on 6 July 2015. Partners welcomed the event and feedback was positive.
CR17e Prevent agenda – new guidance	New guidance on the Prevent agenda is being circulated to the City family of schools including the City of London Academies. A leaflet has been produced for parents and carers regarding the Prevent agenda.	Chris Pelham	10-Jul-2015	Completed – this work has now been completed and the new guidance on the Prevent agenda has been sent to the City of London Family of Schools and the new leaflet has been circulated to parents and carers.
CR17f Review of City of London Safeguarding Policy	A review of the City of London Safeguarding Policy will be undertaken with the involvement of the Departmental Safeguarding Champions	Chris Pelham	31-Dec-2015	Target date for completion 31 December 2015
CR17g Preparation for Inspection of Children's Services and Ofsted Inspection Framework	Work is ongoing to prepare for an Ofsted Inspection of Children's Services. Concerns have been raised by The Society of Local Authority Chief Executives (SOLACE), Local Government Association (GLA) and Association of Directors of Children's Services (ADCS) about the current Ofsted inspection	Chris Pelham	31-Mar-2016	An update on the Corporate Safeguarding Policy will be presented to the Safeguarding sub committee on 25 September 2015

	framework regarding the lack of flexibility and understanding of local demographics and service needs. No Local Authority has been assessed as outstanding since the inspection framework was revised almost 2 years ago.			
--	---	--	--	--

Risk No. & Title	Risk Description (Cause, Event, Impact)	Risk Owner	Current Risk Rating & Score	Risk Update	Target Risk Rating & Score	Target Date	Risk Trend
CR14 Funding Reduction Page 43	<p><b>Cause:</b> Reduced funding from Central Government.</p> <p><b>Event:</b> Reduced funding available to the City Corporation.</p> <p><b>Effect:</b> City Corporation will be unable to maintain a balanced budget and healthy reserves in City Fund, significantly impacting on service delivery levels.</p>	Peter Kane	<p>6</p>	The financial strategy already addresses this risk for City Fund. Following the service based review and inclusion of these savings in budget estimates, the City Fund (non-Police) remains in balance or close to breakeven across the period. Savings begin to be reflected in the budget for 2015/16, approved by the Court, with full impact by or before 2017/18. There are risks around the implementation of the saving proposals and the achievement of savings will be monitored by the Efficiency and Performance	<p>4</p>	31-Mar-2018	↔

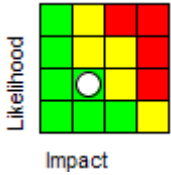
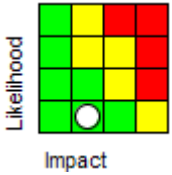
				<p>Sub Committee on a regular basis. As savings proposals are implemented, this risk will ultimately reduce further to GREEN. The MTFP currently anticipates the Revenue Support Grant will reduce to £2m by 2019/2020. In the summer budget, the Chancellor announced overall reductions that are less steep than forecast in the March budget. We do not yet know how this affects us until after the comprehensive spending review in the autumn, but we know the deficit reduction programme is over a longer period and the squeeze has eased a little.</p> <p>Further significant cuts are likely to Home Office Funding for Police services over the next four years as a result of the Spending Review. The separate review of Police Funding Formula may result in a further reduction. The medium</p>			
--	--	--	--	---	--	--	--



				term financial strategy is being updated to address these likely reductions but cannot be finalised until the outcome of the SR and Formula Review is known in late November/December.			
--	--	--	--	--	--	--	--

Action Code & Title	Action Description	Action Owner	Due Date	Action Update
CR14a Scrutiny by the Efficiency Board and Efficiency and Performance Sub-Committee.	Scrutiny of the achievement of savings by the Efficiency Board and Efficiency and Performance Sub-Committee.	Caroline Al-Beyerty	31-Mar-2016	First Departmental SBR Monitoring report provided to May 15 EPSC. Quarterly cycle of reporting agreed for remainder of 2015/16.
CR14b SBR implementation.	SBR implementation continues with cross departmental workstreams to identify further efficiencies in strategic asset management, income generation, and reviews of grants and hospitality.	Caroline Al-Beyerty	31-Mar-2016	Progress is monitored by EPSE in full. Grants renew is complete now more to implement. Recommendations made. Corporate Finance are liaising closely with Police finance team.
CR14c Police Savings proposals.	Police Savings proposals to be quantified and validated by September 2015.	Caroline Al-Beyerty	30-Sep-2015	

CR14d SBR – Savings proposals.	SBR implementation in progress– savings proposals identified that restore the budget to a balanced position across the medium term.	Caroline Al-Beyerty	12-Mar-2015	ACTION COMPLETED.
CR14e Robust financial planning.	Robust financial planning.	Caroline Al-Beyerty	12-Mar-2015	ACTION COMPLETED.
CR14f Monitoring of delivery of savings.	Robust monitoring of delivery of savings proposals – undertaken by Head of Finance, Projects.	Paul Nagle	31-Mar-2016	First round of monitoring complete, 2nd round to commence by end of June 2015.
CR14g Scrutiny by the Efficiency Board and Efficiency and Performance Sub-Committee.	Scrutiny by the Efficiency Board and Efficiency and Performance Sub-Committee.	Caroline Al-Beyerty	12-Mar-2015	ACTION COMPLETED.

Risk No. & Title	Risk Description (Cause, Event, Impact)	Risk Owner	Current Risk Rating & Score	Risk Update	Target Risk Rating & Score	Target Date	Risk Trend
<b>CR16 Information Security</b>	<b>Cause:</b> Breach of IT Systems resulting in unauthorised access to data by internal or external sources. Officer/ Member mishandling of information.	Graham Bell	 4	Mandatory training programme now complete. Structure of policies and guidelines due to be signed off by the IT Steering Group on 1 September 2015.	 2	31-Jan-2016	↔

	<p><b>Event:</b> Cyber security attack – unauthorised access to COL IT systems. Loss or mishandling of personal or commercial information.</p> <p><b>Effect:</b> Failure of all or part of the IT Infrastructure, with associated business systems failures. Harm to individuals, a breach of legislation such as the Data Protection Act 1988. Incur a monetary penalty of up to £500,000. Compliance enforcement action. Corruption of data. Significant reputational damage.</p>						
--	---	--	--	--	--	--	--

Action Code & Title	Action Description	Action Owner	Due Date	Action Update
CR16a Review and refresh policy	Review and refresh existing policy around cybersecurity and technology infrastructure risk in partnership with Agilisys.	Christine Brown	30-Sep-2015	Final version to be agreed at IT Steering group on 1 September 2015, and then Summit Group.
CR16b Promote Data Security training	Actively promote Data Security training and Responsible for Information training plan to be developed and deployed.	Christine Brown; Daniel Mckee	30-Sep-2015	Campaign to ensure colleagues complete mandatory Data Protection Act 1998 and responsible for information courses by end of April 2015. Next steps: Ensure HR inform managers that these courses are mandatory for all new joiners, and that completion should be monitored.
CR16c Central monitoring and guidance.	Ensuring departments comply with the DPA and FOIA, within a corporate policy and compliance	Michael Gasson	12-Mar-2015	ACTION COMPLETED. Draft Internal Audit report states compliance level 'Substantial'.

	framework, via an Access to Information Network (AIN); that guidance is provided, and compliance is monitored.			
CR16d Data Protection awareness raising.	Biannual awareness raising campaigns, including posters, screensavers, tables talkers, and key guidance emails to all staff. (May and November)	Daniel Mckee	12-Mar-2015	ACTION COMPLETED.
CR16e Mandatory online training and Data Protection presentations for staff	Mandatory online training for all staff and rolling program of tailored DPA training presentations for all staff, and to Members on request.	Daniel Mckee	12-Jul-2015	ACTION COMPLETED.
CR16f Technical Solutions Officer.	Appointment of Technical Solutions Officer.	Gary Griffin	12-Mar-2015	ACTION CLOSED. There are currently no plans to recruit to this post.
CR16g Investigations process.	Investigations process in place.	Graham Bell	12-Mar-2015	ACTION COMPLETED.

## Top red departmental risks

Code	Title	Current Rating	Page no
<b>DCCS PE 002</b>	Failure to deliver expansion of Sir John Cass Foundation Primary School to 2 form entry in September 2016	24	1
<b>CCS SMT 004</b>	Successful implementation of Oracle OPN	16	2
<b>GSMD EF 001</b>	Failure to Secure Lease Renewal of Sundial Court in 2020	16	4
<b>GSMD FN 001</b>	Ability to Deliver a Balanced and Sustainable Model over the School's Business Cycle	16	5
<b>MCP-EH 001</b>	Air Quality	16	8
<b>MCP-NS 001</b>	Workplace Traffic Management	16	10
<b>MCP-SM 001</b>	HGV Unloading Operations	16	13
<b>OSD 003</b>	Delivering the Departmental Road Map Projects and Programmes	16	14
<b>OSD 005</b>	Animal, Plant and Tree Disease	16	15
<b>OSD NLOS 008</b>	Hampstead Heath Bathing Ponds	16	16
<b>SUR SMT 005</b>	Recruitment and retention of property professionals	16	17
<b>SUR SMT 009</b>	Failure of implementation and management of the Oracle Property Management System	16	19

Page 49

Addendum to Appendix 2

<b>TC TCO 01</b>	Staff shortage and Capacity	6	1
------------------	-----------------------------	---	---

This page is intentionally left blank



# Top red departmental risk register

Generated on: 24 August 2014

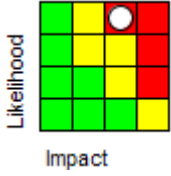
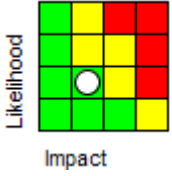
Rows are sorted by Risk Score

Code & Title: CCS SMT SMT risks 1 DCCS PE People Division 1 GSMD EF GSMD Estates and Facilities 1 GSMD FN GSMD Financial 1 MCP-EH Environmental Health Risk Register 1 MCP-NS New Spitalfields Risk Register 1 MCP-SM Smithfield Risk Register 1 OSD Department of Open Spaces Risk Register 2 OSD NLOS Hampstead Heath, Queens Park & Highgate Wood 1 SUR SMT SMT risks 2

Risk No. & Title	Risk Description (Cause, Event, Impact)	Risk Owner	Current Risk Rating & Score	Risk Update	Target Risk Rating & Score	Target Date	Risk Trend
DCCS PE 002 Failure to deliver expansion of Sir John Cass Foundation Primary School to 2 form entry in September 2016	<p><b>Cause</b> Expansion not delivered</p> <p><b>Event</b> Building project not completed</p> <p><b>Effect</b> Lack of first choice school places for City children</p>	Ade Adetosoye	<p>24</p>	Attempts to achieve the target are ongoing.	<p>2</p>	18-Aug-2015	↑

Action Code & Title	Action Description	Action Owner	Due Date	Action Update
DCCS PE 002a Tripartite meetings	Tripartite meetings take place between the Sir John Cass Foundation, Sir John Cass Foundation School Board of Governors and the City of London have taken place but no further meetings have been scheduled.	Chris Pelham	30-Sep-2015	Tripartite meetings have been held to discuss options for delivering additional school places. These meetings have been suspended due to the nonattendance by representatives of the Sir John Cass Foundation.
DCCS PE 002b Discussions with Comptroller and City Solicitor	The Sir John Cass Foundation	Chris Pelham	30-Sep-2015	The options for expansion and the issues regarding the Sir John Cass Foundation have been referred to the Comptroller and City Solicitor

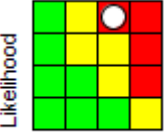

Page 52

Risk No. & Title	Risk Description (Cause, Event, Impact)	Risk Owner	Current Risk Rating & Score	Risk Update	Target Risk Rating & Score	Target Date	Risk Trend
CCS SMT 004 Successful implementation of Oracle OPN	<p><b>Cause</b> – Oracle OPN is replacing the Manhattan commercial property management and rent system</p> <p><b>Event</b> – Implementation of new system</p> <p><b>Effect</b> – If the application does not function as planned and/or the data migrated from Manhattan is of poor quality there is a risk that commercial income will not be invoiced on the due dates.</p>	Martin Howe	 <p>16</p>	Excellent progress has been made in processing and clearing the backlog of work (from mid-February). Data cleansing activities continue and other adjustments are being made as issues arise. All efforts have been made to ensure that accounts are accurate and billed in	 <p>4</p>	01-Oct-2015	↔



				accordance with the terms of leases/licences etc. Work is now progressing in documenting OPN processes to build a knowledge base for the system.			
--	--	--	--	--	--	--	--

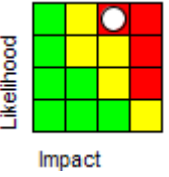
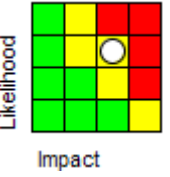
Action Code & Title	Action Description	Action Owner	Due Date	Action Update
C&CS SMT 004a Migrated data needs significant cleansing	Migrated data was poor in quality and impacted on accurate billing and reporting	Martin Howe	01-Oct-2015	Data continues to be cleansed and updated
C&CS SMT 004b Adjust migrated accounts to ensure accurate billing	Certain billing information requires changing to ensure that accounts are billed in accordance with the legal agreements	Martin Howe	01-Oct-2015	Billing adjustments are continuing as issues arise
C&CS SMT 004c Document procedures to generate knowledge base	Very little documentation exists as user manuals. New documentation needs to be produced to act as a definitive user guide and single reference point	Martin Howe	01-Nov-2015	Drafting of process documentation is progressing

Risk No. & Title	Risk Description (Cause, Event, Impact)	Risk Owner	Current Risk Rating & Score	Risk Update	Target Risk Rating & Score	Target Date	Risk Trend
GSMD EF 001 Failure to Secure Lease Renewal of Sundial Court in 2020	<p><b>Cause:</b> Sundial Court , (the School's student accommodation), is owned by a private landlord, who currently leases the building to the School. Lease expires in 2020.</p> <p><b>Event:</b> Landlord may not want to renew the lease to the School as there may be better development potential elsewhere. Alternative specialist music student accommodation might not be found.</p> <p><b>Impact:</b> Loss of on-campus student accommodation for 177 students. Loss of student services and offices. Loss of student union facility and rehearsal room. Risk of reduced interest in students choosing GSMD if there is no onsite accommodation available.</p>	Michael Dick	 Likelihood Impact 16	Legal opinion on lease renewal terms obtained. Alignment of repairs and maintenance regime with lease terms. Contact and dialogue with landlord's agent on issues relating to lease renewal. Engagement with City Surveyors on action plan. Student accommodation strategy in development.	 Likelihood Impact 12	05-Apr-2016	↔

Action Code & Title	Action Description	Action Owner	Due Date	Action Update
GSMD EF 001a Dilapidations Survey	Commissioning of specialist dilapidations survey	Michael Dick	05-Apr-2016	Specialist dilapidations surveyor engaged

GSMD EF 001b Accommodation Alternative	Search for availability of alternative student accommodation	Michael Dick	05-Apr-2016	Meeting with Unite/specialist student accommodation provider
GSMD EF 001c City Surveyor Liaison	Engagement with City Surveyor on action plan	Michael Dick	05-Apr-2016	In progress
GSMD EF 001d Student Accommodation Strategy	Develop long-term student accommodation strategy	Michael Dick	05-Apr-2016	Draft accommodation strategy in development

D  
S  
S  
S

Risk No. & Title	Risk Description (Cause, Event, Impact)	Risk Owner	Current Risk Rating & Score	Risk Update	Target Risk Rating & Score	Target Date	Risk Trend
GSMD FN 001 Ability to Deliver a Balanced and Sustainable Model over the School's Business Cycle	<p><b>Cause:</b> Substantial drop in income. Pressures on expenditure. Service Based Review funding cuts of £1m in 17/18. Local risk funding to the School is planned to reduce from over £8m in 2013/14 to £5.3m in 2017/18. Failure to gain additional funding from HEFCE.</p> <p><b>Event:</b> If no action is taken, the School's annual deficit will rise to £3.2m by 2017/18.</p> <p><b>Impact:</b> This is not a sustainable position and the Higher Education Funding Council for England</p>	Barry Ife	 <p>16</p>	Risk 5.2 on Departmental Risk Register The School and the CoL are in direct discussions with HEFCE. Up to date communication and reporting to the Board, CoL and HEFCE. Ongoing discussion and negotiation to effect funding model. Continual review and management of the School's business model. On current funding levels, the School's longterm	 <p>12</p>	31-Jan-2016	↔

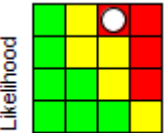
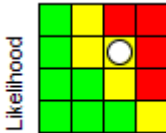
(HEFCE) have been made aware.

financial model is unsustainable. This has been materially exacerbated by the City's Service Based Review (SBR) target, reducing City funding to the School by £1m in 2017/18. Over the last year the School has engaged with both HEFCE and the City to determine a strategy that will re-balance the model. Although a number of options have been discussed, these discussions with the School's primary funders are crucial in determining future strategy. Discussions have been initiated with HEFCE concerning the possibility of increased public funding as part of its review of institution-specific targeted allocations (RISTA) scheduled for 2015/16. in the interim the School is working to ensure that the quality of its teaching and the strength of its brand holds within the current volatile

				environment. The School has put together a plan of action for investing in its capabilities to ensure that it retains its leading position in a competitive environment.			
--	--	--	--	--	--	--	--

Action Code & Title	Action Description	Action Owner	Due Date	Action Update
GSMD FN 001A Securing School Funding Page 57	<p>Tuition fee income is planned to grow from £7.5m in 2013/14 to £9.4m in 2017/18.</p> <p>Grants and contracts are also planned to grow, but the School has approached HEFCE for an additional grant to bridge the funding gap caused by the planned reduction in City funding to the School.</p> <p>All other forms of operating income (short courses and summer schools, enterprise and space hire) will also be maximised and costs reduced to an absolute minimum.</p> <p>Grow income from tuition fees Seek additional public funding to cover reduced City funding, specifically from HEFCE following their review of institution-specific allocations (2015)</p>	Barry lfe	31-Jan-2016	Ongoing, detailed update to follow

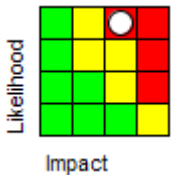
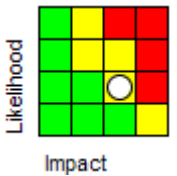
GSMD FN 001B Identify potential savings	Reduce cost to bare minimum compatible with delivering the curriculum to the required specification and maintaining a competitive level of student experience Consider reductions in the range of high-cost theatre-based disciplines (acting, technical theatre, opera and musical theatre)	Barry lfe	31-Mar-2016	Ongoing, detailed update to follow
GSMD FN 001C Potential merger with another institution	Explore options for merger with a larger, better-funded institution in London, the UK or overseas	Barry lfe	31-Mar-2016	Ongoing, detailed update to follow

Risk No. & Title	Risk Description (Cause, Event, Impact)	Risk Owner	Current Risk Rating & Score	Risk Update	Target Risk Rating & Score	Target Date	Risk Trend
<b>MCP-EH 001 Air Quality</b>	<b>Cause:</b> Poor air quality in the city caused predominantly by traffic pollution. (Air Quality Limit values are legally binding EU parameters that must not be exceeded. Limit values are set for individual pollutants and are made up of a concentration value, an averaging time over which it is to be measured.) <b>Event:</b> Failure to meet Air Quality	Jon Avern	 Likelihood Impact	16 The current systems in place allow the City to demonstrate that it is taking sufficient effective action to help the government and the GLA to meet air quality Limit Values	 Likelihood Impact	12 01-Jan-2018	↔

	<p>limit values in the City by the prescribed dates set by the EU.</p> <p><b>Effect:</b> A fine of unknown amount and the associated reputational damage to the City of London.</p> <p>Poor air quality is also a significant public health issue for the City of London as a small number of the population are more vulnerable to the effects of air pollution where exposure to pollution can exacerbate existing health conditions including cardiovascular and respiratory disease. This can lead to restricted activity, hospital admissions and even premature mortality.</p>						
--	--	--	--	--	--	--	--

Action Code & Title	Action Description	Action Owner	Due Date	Action Update
MCP-EH 001a Implement Actions	Implement the actions set out in the City Air Quality Strategy 2015 – 2020.	Steve Blake	31-Dec-2019	This is currently being progressed.
MCP-EH 001b Ensure Compliance	Ensure the City Corporation complies with the legal obligation to review and assess air quality as detailed in the Environment Act 1995.	Steve Blake	30-Apr-2015	R. Calderwood reports: Annual reports are submitted for approval to Defra / GLA in April each year.

MCP-EH 001c	Review the designation of the City as an Air Quality Management Area (AQMA) due to ongoing levels of pollution.	Steve Blake	31-Dec-2015	R. Calderwood reports: The City was declared an AQMA in 2001. The designation is reviewed every 3 years in line with statutory obligations.
MCP-EH 001d	Work with the Mayor of London to ensure actions taken to improve air quality are in line with GLA / TfL plans	Steve Blake	31-Dec-2015	R. Calderwood reports: This is progressing - the GLA hasn't made any decisions on awarding Cleaner Air Borough Status to any London authority yet. we have submitted sufficient information to demonstrate compliance with their requirements.

Risk No. & Title	Risk Description (Cause, Event, Impact)	Risk Owner	Current Risk Rating & Score	Risk Update	Target Risk Rating & Score	Target Date	Risk Trend
MCP-NS 001 Workplace Traffic Management	<p><b>Cause:</b> Over 200 forklift trucks operate on the New Spitalfields Market site.</p> <p><b>Event:</b> There is a serious risk of injury or death of a pedestrian if vehicle movements in this constrained space are not appropriately managed and controlled.</p> <p><b>Effect:</b> An accident involving a pedestrian and a vehicle which resulted in a serious injury or fatality could result in prosecution, a fine, reputational damage for the City and have an adverse impact on the operation and sustainability of</p>	Sidney Brewer	 16	A traffic management plan is currently in place. The market constabulary monitor fork lift operator behaviours and withdraw permits when required. They also issue penalty points and an accumulation of points will lead to a suspension or cancellation of the permit to operate on the common parts.	 8	02-Jan-2017	↔

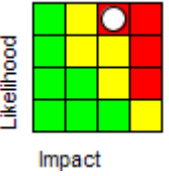
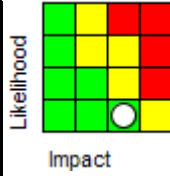


	the service.						
--	--------------	--	--	--	--	--	--

Action Code & Title	Action Description	Action Owner	Due Date	Action Update
MCP-NS 001a Develop plan	Formulate, develop and agree a short, medium and long term plan to improve the management of workplace transport at New Spitalfields Market.	Nigel Shepherd	30-Apr-2015	This action has been completed.
MCP-NS 001b Mark Forklift Crossing Points	Marked Fork lift truck crossing points on pedestrian walkway from stands to roadways.	Sidney Brewer	30-Sep-2015	N. Shepherd reports: Roadways 1 and 2 written to as of 15/5/2015 to finalise location/number/size.
MCP-NS 001c Increase Constabulary Targets	Increase in targets for constabulary.	Nigel Shepherd	01-May-2015	This action has been completed.
MCP-NS 001d Nominate Training Body	To nominate/Appoint one approved induction/training body for all FLT training activities.	Sidney Brewer	30-Oct-2015	This is currently with the Central Health & Safety Team and is taking longer to progress than first thought. This is mainly due to the fact that this isn't a service being procured directly for the City of London.
MCP-NS 001e Ensure Permits are carried	Fork lift truck operators to have their permits to operate readily available at all times.	Nigel Shepherd	01-Jun-2015	N. Shepherd reports that: Implemented and now part of routine operational enforcement activity
MCP-NS 001f All Visitors in Hi Vis	All staff and customers to wear hi-vis vests.	Nigel Shepherd	01-May-2015	N. Shepherd reports that: Implemented and now part of routine operations. Comment - still selling high number of Hi-Vis to visitors routinely in a high profile campaign

MCP-NS 001g Increase Forklift Sanctions	Increase specified breaches of non-compliance with H&S policies	Nigel Shepherd	01-Jun-2015	This action has been completed.
MCP-NS 001h Impose Financial Penalties	Impose financial penalty on tenants when FLT operators are suspended/allocated points	Sidney Brewer	01-Sep-2015	N. Shepherd reports that: Agreement is reached on the principle, but this will need to be included in the lease to enable the market to act upon. Needs new lease in place with a working manual clause and the work manual itself agreed and signed off.
MCP-NS 001i Train Managers In Forklift Safety	A member of staff from all tenants to be nominated and trained in FLT safety procedures.	Sidney Brewer	01-Sep-2015	N. Shepherd stated that: Agreement is reached on the principle, but this needs to be in the lease to be meaningful. C&CS have said this should be possible to achieve under renewal process
MCP-NS 001j Create Time Segregation	Artic Time Segregation and No Tolerance in market hall.	Sidney Brewer	01-Feb-2016	This is part of the longer term plan which will be implemented in 2016.
MCP-NS 001k Install Barrier System	Controlled barriers entry system for pedestrians and vehicles.	Sidney Brewer	01-Oct-2018	This is part of the long term plan to be implemented in 2018.
MCP-NS 001l Segregate Walkways	Create segregated walkways in crossroads.	Sidney Brewer	01-Feb-2016	N. Shepherd has stated that: Consultant engaged for study into all areas as preamble to long term actions.
MCP-NS 001m Segregate Main Walkways	Segregated walkways outside tenants stands.	Sidney Brewer	01-Mar-2016	N. Shepherd has stated that: Consultant engaged for study into all areas as preamble to long term actions.

MCP-NS 001n Prohibit Forklifts	No fork lift truck movements in market pavilion during trading hours.	Sidney Brewer	02-Oct-2017	N. Shepherd has stated that: Consultant engaged for study into all areas as preamble to long term actions.
--------------------------------------	---	---------------	-------------	--

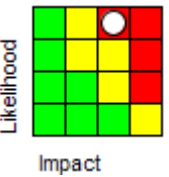
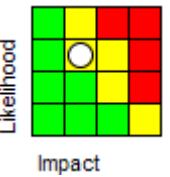
Risk No. & Title	Risk Description (Cause, Event, Impact)	Risk Owner	Current Risk Rating & Score	Risk Update	Target Risk Rating & Score	Target Date	Risk Trend
MCP-SM 001 HGV Unloading Operations  Page 63	<p><b>Cause:</b> A lack of suitable and sufficient training and adequate management controls in relation to Heavy Goods Vehicle banksman activities undertaken by staff employed by Smithfield Market tenants.</p> <p><b>Event:</b> Serious or fatal injury to members of the public, market staff and other service users caused by uncontrolled or unguided reversing vehicles.</p> <p><b>Effect:</b> Realisation of this risk could result in a prosecution, fine and reputational damage for the City.</p>	Robert Wilson	 16	The market constabulary are currently monitoring these areas as part of their routine patrols and are halting any unsafe acts they observe.	 4	31-Dec-2015	↔

Action Code & Title	Action Description	Action Owner	Due Date	Action Update
MCP-SM 001a Traffic management audit	Commission Freight Transport Association to conduct audit and prepare a risk assessment relating to whole site traffic management and unloading issues.	Robert Wilson	15-Dec-2015	P. Spooner reports: All risk assessments have been revised and updated. The tenants have been provided with the H&S report finalized in 2014. The Working Manual is now complete and with the SMTA. The FLT Policy has been reviewed by the HoS and remains with the SMTA for comment.

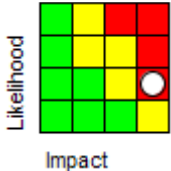
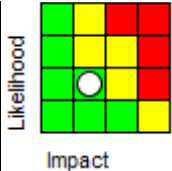
				Smithfield is in receipt of the PowerPoint presentation of the FTA (presented 10th July) and initial recommendations document. This will be subject of discussions meeting with internal partners on 19/8, before progressing to a multi-agency/partnership workshop. Local measures resulting from H&S Audit by COL H&S are now in place and will be implemented in line with above. The maintenance team have installed the recommended equipment from the report by John Smith and Oliver Sanandres. HR Health and Safety officer for use in the unloading of product onto the Market
MCP-SM 001b Loading bay risk assessment	Loading bay risk assessment to be reviewed and issued to market tenants.	Robert Wilson	02-Mar-2015	P. Spooner reports: All risk assessments have been revised and updated. The tenants have been provided with the H&S report finalized in June 2014.

Risk No. & Title	Risk Description (Cause, Event, Impact)	Risk Owner	Current Risk Rating & Score	Risk Update	Target Risk Rating & Score	Target Date	Risk Trend
OSD 003 Delivering the Departmental Road Map Projects and Programmes	<p><b>Causes:</b> Lack of appropriate skill sets to deliver projects; cultural resistance; initial scoping of project outcomes and timescales inaccurate</p> <p><b>Event:</b> Department is unable to deliver its roadmap projects and programmes in agreed timescales or achieve agreed outcomes</p> <p><b>Impact:</b> Alternative savings undertaken which may not be consistent with achieving cultural change or improving outcomes.</p>	Sue Ireland	<p>16</p>	Initial Project and Programme training completed. Further training on stakeholder management in development.	<p>2</p>	01-Apr-2016	↑

Action Code & Title	Action Description	Action Owner	Due Date	Action Update
OSD 3 a Departmental roadmap	Roadmap sets out departmental projects and key corporate projects with timescales and RAG status	Esther Sumner	31-Mar-2015	Roadmaps now complete and being regularly updated.
OSD 3 b Opportunity Outlines	All roadmap projects start with an opportunity outline	Esther Sumner	01-Apr-2016	Opportunity outline process initiated and continues, action considered completed.
OSD 3 c Departmental training	Training for the Departmental Management Team and their direct reports	Esther Sumner	30-Apr-2015	Training complete.

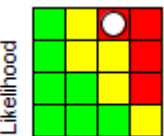

Risk No. & Title	Risk Description (Cause, Event, Impact)	Risk Owner	Current Risk Rating & Score	Risk Update	Target Risk Rating & Score	Target Date	Risk Trend
OSD 005 Animal, Plant and Tree Disease	<p><b>Causes:</b> Inadequate biosecurity, buying of infected trees, plants or cattle, spread of windblown Oak Processionary Moth (OPM ) from adjacent sites</p> <p><b>Event:</b> Sites become infected by animal, plant or tree diseases</p> <p><b>Impact:</b> Public access to sites restricted, animal culls, tree decline, reputational damage, cost of control of invasive species, risk to human health from OPM or other invasives</p>	Sue Ireland	 <p>16</p>	OPM has now been confirmed at Hampstead Heath. Officers continue to work with the Forestry Commission to control OPM.	 <p>6</p>	01-Apr-2016	↔

Action Code & Title	Action Description	Action Owner	Due Date	Action Update
OSD5 a Monitoring of OPM	Pheromone traps in place, liaison with Forestry Commission task force	Sue Ireland	01-Apr-2016	Pheromone traps in place.
OSD5 b Treatment of any OPM sites	Treatment will be depend on lifestyle of the OPM but to be undertaken as early as possible	Andy Barnard; Gary Burks; Martin Rodman; Paul Thomson; Bob Warnock	01-Apr-2016	OPM has been found at NLOS. We are engaging with the Forestry Commission and specialist contractors are removing the nests.
OSD5 c Cattle biosecurity	Movement of cattle to be controlled to reduce risk of disease	Andy Barnard; Paul Thomson	01-Apr-2016	Biosecurity protocol in place
OSD5 d Plant and tree procurement	Sourcing to be controlled to minimise spread of disease	Andy Barnard; Gary Burks; Martin Rodman; Paul Thomson; Bob Warnock	01-Apr-2016	Hampstead Heath have engage with Ponds Project contractors about controls required for trees and plants brought to site

Risk No. & Title	Risk Description (Cause, Event, Impact)	Risk Owner	Current Risk Rating & Score	Risk Update	Target Risk Rating & Score	Target Date	Risk Trend
OSD NLOS 008 Hampstead Heath Bathing Ponds	<b>Cause:</b> Lack of suitably experienced and qualified lifeguarding staff at Hampstead Heath Bathing Ponds. Members of the public swimming in unauthorised areas. Swimming outside of designated zones. Swimmers fail to pay attention to acclimatisation requirements. <b>Event:</b> Unable to effect safe rescue	Bob Warnock	 Likelihood Impact	National Water Safety Programme Management training module will be delivered to relevant staff. Qualified lifeguards at pond facilities train on a regular basis. Signage available and abundant.	 Likelihood Impact	01-Apr-2016	↔

	of swimmers. Death or serious injury of swimmers in ponds. <b>Impact:</b> Death or injury to members of the public or staff who enter water. Possible legal challenge. Emotional impact on staff. Reputational risk.						
--	---	--	--	--	--	--	--

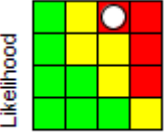

Action Code & Title	Action Description	Action Owner	Due Date	Action Update
OSD NLOS 008 a Training	Training for lifeguards	Bob Warnock	31-Mar-2016	Training needs reviewed and actioned
OSD NLOS 008 b Signage	Appropriate signage at ponds	Bob Warnock	31-Mar-2016	Signage in place
OSD NLOS 008 c Safety equipment	Safety equipment accessible at ponds	Bob Warnock	31-Mar-2016	Safety equipment in place and checked

Risk No. & Title	Risk Description (Cause, Event, Impact)	Risk Owner	Current Risk Rating & Score	Risk Update	Target Risk Rating & Score	Target Date	Risk Trend
<b>SUR SMT 005 Recruitment and retention of property professionals</b>	<b>Cause:</b> A strong property and construction market <b>Event:</b> Increasingly attractive remuneration packages offered elsewhere <b>Impact:</b> Increased vacancies, objectives unachieved or delivered	Peter Bennett	 Likelihood Impact <b>16</b>	This risk identifies the continuing turnover of staff as a result of the strong property market. The department is developing strategies specific to the department that have a	 Likelihood Impact <b>4</b>	31-Mar-2016	↑

	late, reduced customer satisfaction			<p>particular focus on talent management, reward and retention. There is also a focus on identify projects or work where value can be added by outsourcing.</p> <p>The department now has an action plan in place which includes the introduction of career grading and individual reward packages.</p>			
--	-------------------------------------	--	--	---	--	--	--

Action Code & Title	Action Description	Action Owner	Due Date	Action Update
SUR SMT 005 Adopt and Change Approach	Encourage CoL to adapt and change the approach to Reward and Earnings Package	Peter Bennett	30-Apr-2016	progressing
SUR SMT 005a Develop Workforce Plan	Establish strategies specific to the department that have a particular focus on talent management, reward and retention	Peter Bennett	30-Apr-2016	Management team meetings are underway with HR. HR are identifying people and teams that would face loss and a range of strategies to be put into place to limit the effect. Focusing on the need to recruit and retain.



Risk No. & Title	Risk Description (Cause, Event, Impact)	Risk Owner	Current Risk Rating & Score	Risk Update	Target Risk Rating & Score	Target Date	Risk Trend
SUR SMT 009 Failure of implementation and management of the Oracle Property Management System	<p><b>Cause:</b> Implementation and subsequent management of Oracle Property module to meet business needs</p> <p><b>Event:</b> Inappropriate technological solution or unsuccessful project management or failure to implement an appropriate management framework</p> <p><b>Impact:</b> Unable to manage property portfolio / loss of income and poor property maintenance</p>	Nicholas Gill	 16	Open issues have been progressed. However there are still some unresolved issues on service Charge Solution and OPN reports. The five elements that are being finalised include 1) Defects Resolution, 2) Service Charge, 3) Argus Interface, 4) Archibus Interface and 5) OPN Reports. The programme is due to be completed mid-September 2015.	 8	30-Sep-2015	↔

Page 69

Action Code & Title	Action Description	Action Owner	Due Date	Action Update
SUR SMT 009a Monitor Staff Resources	Monitor staff resources to manage business as usual tasks and project	Nicholas Gill	30-Sep-2015	Senior Principal Surveyor assigned 100% to Oracle OPN project to ensure successful completion.
SUR SMT 009b Replace core Manhattan functions	Replace core Manhattan functions of rent, leases management and service charge recovery	Nicholas Gill	30-Sep-2015	Manhattan no longer in use switched to OPN.

<p>SUR SMT 009c Ensure efficient use and future management of system -</p>	<p>Ensure efficient use and future management of system- implement Asset Management Information System Ensure Data Loader is able to update projects</p>	<p>Nicholas Gill</p>	<p>30-Sep-2016</p>	<p>Business as usual model, still to be addressed.</p>
--	--	----------------------	--------------------	--



# TC TCO 01 Staff shortage and Capacity (previous risk no CR18)

Generated on: 21 August 2015

Code & Title: TC TCO Town Clerk's Office 1

Risk No. & Title	Risk Description (Cause, Event, Impact)	Risk Owner	Current Risk Rating & Score	Risk Update	Target Risk Rating & Score	Target Date	Risk Trend
TC TCO 01 Staff shortage and Capacity (previous risk no CR18) Page 71	<p><b>Cause</b> – A combination of changes to economic, legislative environment or employment market</p> <p><b>Event</b> – Critical loss of capacity in business critical roles, impacting our ability to achieve our strategic aims/service provision</p> <p><b>Effect</b> – Inability to recruit and retain business critical staff</p>	Chrissie Morgan	<p>6</p>	<p>This risk was reviewed by the Corporate HR SMT on 20 August 2015 and there is no change to the risk assessment level.</p> <p>All departments have been asked to form a workforce planning group and complete a workforce plan by end of July. These plans have now been received and are currently being analysed. The plans include forecasting the risk of service critical jobs or single points of failure and an action plan to manage that risk. Corporate analysis of the plans will result in the prioritisation of the review of the key policies</p>	<p>4</p>	31-Mar-2017	↔

				which can support the management and mitigation of the risk. Early analysis has shown some key themes for departments - succession planning - and corporately - flexibility of pay. These will be further analysed over the coming weeks, identifying more research if necessary.			
--	--	--	--	---	--	--	--

Action Code & Title	Action Description	Action Owner	Due Date	Action Update
TCO 01A Departmental workforce planning groups and plans	Establish departmental workforce planning groups to act as a focus for departmental workforce planning and produce a workforce plan	Chrissie Morgan	31-Jul-2015	This action is now complete
TC TCO 01B Corporate analysis of departmental workforce plans	Analyse departmental workforce plans to establish key themes, and prioritise the review of key policies which can support management and mitigate risks associated with the workforce.	Chrissie Morgan	31-Dec-2015	Early analysis has shown that succession planning and the flexibility of pay some to be common themes that have been identified

<b>Committee(s)</b>	<b>Dated:</b>
Audit and Risk Management Committee	17/09/2015
<b>Subject:</b> Anti-Fraud & Investigations Up-date Report	<b>Public</b>
<b>Report of:</b> Chamberlain	<b>For Information</b>

## Summary

This report provides Members with an update of our anti-fraud and investigation activity; it also provides an analysis of the cases investigated during 2015/16 to date.

A successful housing benefit prosecution was secured in the Central Criminal court, resulting in a 20 week custodial sentence, suspected for two years, along with the repayment of £72,377 fraudulently claimed benefit. Positive publicity was received in this case following a publication in the Southwark News.

Three City Corporation properties that had been illegally sub-let and one that had been obtained by deception have been possessed and let to those in greatest need. A further two cases are currently in the Crown court awaiting criminal trial and six more cases are with the Comptroller & City Solicitor, five for criminal prosecution action and three for civil recovery action.

The City Corporation's participation in the National Fraud Initiative exercise has identified fraud with a value in excess of £51,000 from the matches reviewed to-date. Recovery action is in progress where possible. Further reviews are continuing to be undertaken against outstanding NFI matches.

Two corporate frauds referrals and one whistleblowing referral were received and investigated by the team; although the allegations were not substantiated, recommendations were made to strengthen controls where opportunities to commit fraud and exploit weaknesses were identified.

A report - Protecting the London Public Purse (PLPP) 2015 was commissioned by the London Borough Fraud Investigators Group, which benchmarked London boroughs work to tackle fraud across the region against work done in previous years; likewise the report highlighted the current and emerging key fraud risks for London boroughs. The Anti-Fraud & Investigation team will be benchmarking its work and proactive anti-fraud plan against the fraud risks identified in PLPP 2015 and will make changes as necessary in order to ensure that key fraud risks are being adequately examined.

## Recommendation(s)

- Members are asked to note the report

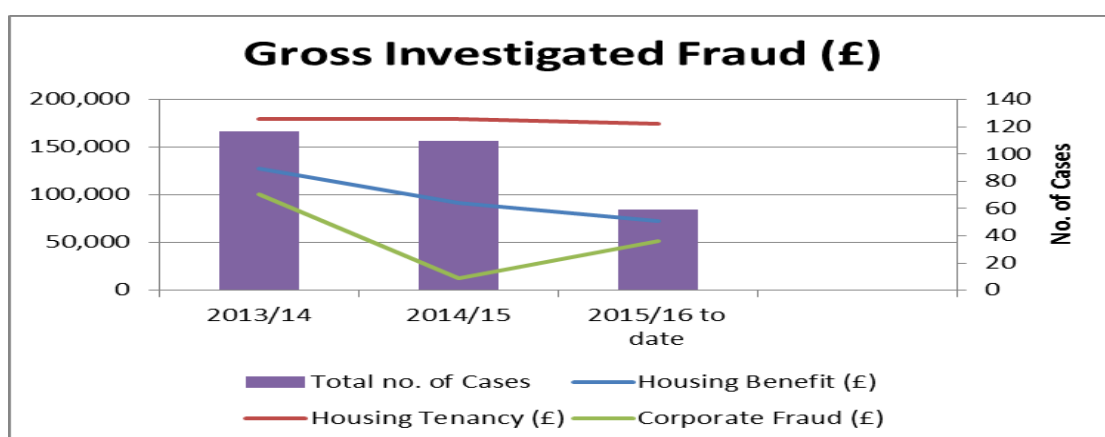
## Main Report

### Background

1. This report updates Members with the key issues arising from anti fraud and investigations work since the last report to Committee in April 2015.

### Investigation Activity Summary

2. The graph below shows a trend analysis of the number of cases investigated during the current reporting year 2015/16, against the previous two years. This shows all fraud types, along with the value of frauds detected for both housing benefit and housing tenancy investigations. The value of corporate fraud investigations are shown where these can be quantified.



3. A detailed housing tenancy fraud caseload report is contained as Appendix 1 to this report.

### Housing Benefit Fraud Prosecution

4. The City of London Corporation recently secured a prosecution at the Central Criminal Court against one of its housing tenants for benefit fraud offences. Investigations found that XX had fraudulently claimed housing benefit, council tax benefit, jobseekers allowance and employment and support allowance from the City Corporation, Southwark Council and the Department for Work & Pensions, over an eight year period by failing to declare she had capital which exceeded the levels permitted for entitlement to benefit. As a result of this fraud, the authorities calculated that XX had been overpaid £72,377 in benefits during the period. XX pleaded guilty to 13 counts of fraud and was sentenced to 20 weeks imprisonment, suspended for two years. The overpayment has been repaid in full, along with £7,500 interest.
5. Following a press release issued by the City's Public Relations office, the case was publicised in the Southwark News, leading to positive publicity for the City of London. A copy of the publication is included at Appendix 2 to this report.

### Housing Tenancy Fraud

6. Three fraudulently sublet City Corporation properties, and one obtained by deception have been recovered so far in this reporting year and are now being let to others in far greater need of housing. A further two cases are currently in the Crown court awaiting criminal trial and six more cases are with the Comptroller & City Solicitor, five for criminal prosecution action and three for civil recovery action.
7. The work of the Fraud Investigator at the City's Avondale Square estate in respect of housing tenancy and benefit fraud has recently been commended by the Area Housing Manager following a review of positive outcomes achieved on the Avondale Square estate.
8. A right to buy fraud has recently been identified by the Anti-Fraud & Investigation team, following a referral from the home ownership officer. The investigation found that the tenant was living away from the property and therefore did not qualify for the right to buy. The right to buy application was refused and we are currently liaising with the Comptroller & City Solicitor to establish whether any further civil or criminal action is suitable.

### **National Fraud Initiative**

9. The Anti-fraud & Investigation team have progressed 314 National Fraud Initiative matches since their release in January this year, covering fraud risk areas including housing tenancy fraud, Council tax fraud and disabled parking permit fraud, no recourse to public funds fraud, pension fraud and duplicate payment errors. Other matches relating to possible benefit fraud, payroll fraud, and direct payment fraud will be reviewed with departmental colleagues throughout the year.
10. A number of successful outcomes have been obtained and are summarised in the table below. A number of successful outcomes have been obtained and are summarised in the table below. The pension fraud outcomes relate to two individuals who had passed away; overpayments were created and further scheduled payments stopped. Council tax fraud outcomes relate to two confirmed fraudulent single person discount claims and the identified duplicate payment related to an invoice that was found to have been paid twice. These overpayments are subject to recovery action by the City Corporation. Identified housing tenancy fraud is valued at £18,000 per investigation.

<b>Fraud type</b>	<b>No. of cases</b>	<b>Value £</b>
Pension Fraud	2	2,125
Council Tax Fraud	2	11,351
Housing Tenancy Fraud (included in tenancy fraud appendix)	2	36,000
Duplicate Payments	1	1,894
<b>Total</b>	<b>8</b>	<b>£51,370</b>

### **Corporate Fraud**

11. A report was received from the financial services division relating to concerns that income amounting to £2,249, from public conveniences in the City had shortfalls over a four day period in May 2015. Investigations found that the City's contractor, responsible for collecting income from the public conveniences, was using the coins emptied from the collection tins for change at other public conveniences as the banks were closed during the bank holiday period. It was identified that this arrangement was not authorised by the City Corporation. The shortfall has been reimbursed and we have been given assurances that the contractor has now ceased this process.
12. A referral was received from the City Police finance team following a review of contractors' payments and timesheets that had identified a potentially serious financial irregularity, including alleged corruption in the sign-off of time sheets and the fraudulent use of a staff member's signature during a period that she was on maternity leave. Enquiries found that the contractor was a highly paid individual and payments to the resourcing supplier had been on hold for over six months, with invoices exceeding £80,000 outstanding. Following an internal audit investigation it was identified that the contractor had not been procured under the Comensura corporate contract and as such controls over the temporary contract were limited and purchase orders had not been raised. No evidence could be found to support that fraudulent timesheets had been submitted, however a breakdown in communication was identified between City Police HR and the procuring division which meant that a reduced hourly rate earlier agreed was not implemented and resulted in the contractor being paid a higher hourly rate than necessary. A number of recommendations were made in relation to our findings to strengthen controls in this area. These have been agreed and are being implemented.

### **Whistleblowing**

13. A whistleblowing referral was received from a member of the public following a visit to the Monument in January 2015. The whistle-blower raised concerns that he and other visitors had not been provided with a receipt during their visit to the Monument. An internal audit investigation was undertaken which identified that on the day of the visit the tills at the monument had crashed and manual income collection arrangements had been implemented. A review of all income received during the period covering the visit was carried out, along with a review of the processes for reconciling and banking of cash income, however we were unable to identify any suspicious transactions. Three minor recommendations were made in relation to our findings, which have been agreed and are due to be implemented.

### **Protecting the London Public Purse (PLLP) 2015 Report**

14. The London Borough Fraud Investigators Group (LBFIG) recently commissioned a pan London report, PLPP 2015, released in July 2015, regarding the region's response to fraud against London boroughs. The authors of the report used data gathered from London boroughs following a comprehensive survey, and utilised publicly available data from previous Protecting the Public Purse reports, produced by the Audit Commission, in



order to benchmark the anti-fraud work and results across London against previous years.

15. The PLPP 2015 report identified that the value of detected fraud committed against London boroughs, during 2014/15 amounted to £73m, an increase of 46 per cent compared to the previous year.
16. PLPP 2015 also identified and recommends several key fraud risks areas for London boroughs to focus resources on in future work plans, these are;
  - Right to buy (RTB) fraud – in excess of 300 cases were identified across London with a value of £26m, with at least 3 per cent of RTB applications being fraudulent.
  - No recourse to public funds (NRPF) fraud – 432 cases were identified with a value of £7m, with NRPF fraud representing one of the most significant fraud types detected by London boroughs.
  - Tenancy Fraud – 1,618 tenancy frauds were detected across London, with two thirds of all illegal sub-letting detected across England being in London boroughs.
17. A successful City Corporation prosecution in the Central Criminal Court last April relating to a tenant who had committed tenancy fraud and NRPF fraud was used as a case study within the PLPP 2015 report, providing further positive publicity of our successful work in the fight against fraud.
18. The Anti-Fraud & Investigation team will be benchmarking its work and proactive anti-fraud plan against the fraud risks identified in PLPP 2015 and will make changes as necessary in order to ensure that key fraud risks are being adequately examined.

## **Conclusion**

19. Internal Audit continues to provide a professional anti-fraud and investigation service, with successful investigations resulting in positive outcomes and positive publicity for the City Corporation. Housing tenancy fraud continues to be a key fraud risk for the City Corporation, evidenced by the outcomes obtained to date and the criminal prosecution and civil cases currently in the crown court or with the Comptroller and City Solicitor.

## **Appendices**

**Appendix 1: Housing Tenancy Fraud Caseload**

**Appendix 2: Press Release – Housing Benefit Fraud**

**Contact:** Chris Keesing, Anti-Fraud Manager  
[chris.keesing@cityoflondon.gov.uk](mailto:chris.keesing@cityoflondon.gov.uk) 020 7332 1278

This page is intentionally left blank

## Appendix 1 – Housing Tenancy Fraud Caseload as at 20/08/2015

Housing Tenancy Fraud Case Referrals	April 2015 to Date	April 2014 to March 2015	April 2013 to March 2014
Referrals received in current year	18	44	28
Cases carried over from previous years <sup>1</sup>	29	14	10
<b>Total</b>	<b>47</b>	<b>58</b>	<b>38</b>
<b>Cases currently under investigation</b>	28	29	11
<b>Cases closed with no further action</b>	4	11	13
<b>Cases with Comptroller &amp; City Solicitor for prosecution</b>	5	5	3
<b>Cases with Comptroller &amp; City Solicitor for civil recovery</b>	3	0	0
<b>Cases where possession order granted</b>	0	0	0
<b>Cases where successful possession gained <sup>2</sup></b>	4	10	10
<b>Cases where successful prosecution action taken</b>	0	2	0
<b>Cases where fraudulent application identified</b>	2	1	1
<b>Right to buy fraud successfully identified</b>	1		
<b>Total</b>	<b>47</b>	<b>58</b>	<b>38</b>
<b>Value where successful possession gained/ right to buy fraud identified <sup>3</sup></b>	<b>£175,000</b>	<b>£180,000</b>	<b>£180,000</b>
<b>Notes:</b>			
<sup>1</sup> Previous year's data shows the position at year end, and is provided for comparative purposes. Cases carried over from previous years do not represent live cases in the current reporting year.			
<sup>2</sup> Cases where successful possession has been gained will be considered for criminal action where suitable, and where offences committed are serious enough to warrant proceedings under the Prevention of Social Housing Fraud Act 2013 and/ or the Fraud Act 2006.			
<sup>3</sup> Successful possession gained value of £18,000 per property sourced from Audit Commission value of national average temporary accommodation costs to Local Authorities for one family. RTB discount value currently £103,000.			

This page is intentionally left blank

## Appendix 1: Press Release – Housing Benefit Fraud Prosecution



AMELIA BURR (13 August, 2015) **CRIME**

### Defendant let off after she paid back money claimed in full with interest

A Bermondsey benefits scammer has been spared jail after she was found guilty of claiming £72,000 in benefits when she had over £80,000 in the bank.

XX, a resident of the Avondale Square Estate just off the Old Kent Road, was found to have fraudulently obtained housing benefit, council tax and job seeker's allowance payments between 2003 to 2013.

The City of London Corporation, which owns the estate, took XX to court when staff discovered she had £84,000 in the bank, which Judge Nicholas Cooke QC said appeared had been paid in by XX's mother to avoid tax. Before sentencing the 51-year-old to 20 weeks' imprisonment suspended for two years, Judge Cooke said: "It is the hypocrisy that is distasteful."

But he added he was prepared to pass a suspended prison sentence because XX had repaid the full amount plus interest, totalling £79,877.33.

The Old Bailey heard how the defendant did not touch the money in the savings account during the fraud and in fact lived a "very modest lifestyle."

Chris Keesing, Anti-Fraud Manager for the City of London Corporation, said: "There is no hiding place for people who commit benefit fraud. It is a myth that benefit fraud is a victimless crime. It is public money that could have gone towards helping someone in genuine need or towards funding cash-strapped public services. I would urge anyone who suspects fraud to report it to the authorities."

This page is intentionally left blank

<b>Committee(s)</b>	<b>Dated:</b>
Audit & Risk Management Committee – For Information Finance Committee - For Information	17/09/2015
<b>Subject:</b> Cyber Security Risks	<b>Public</b>
<b>Report of:</b> Chamberlain	<b>For Information</b>

## Summary

Cyber security and associated risks present a current and continuously evolving risk to the City of London Corporation and the City of London Police. The City Corporation has strengthened its audit activity in this area, drawing on appropriate internal and external expertise.

The Committee received a report in April setting out the cyber fraud risks facing the City Corporation and the City Police. The report summarised the potential vulnerabilities, possible audit activity and action being taken by management to minimise the threat of successful fraud. This report summaries the current position for the City Corporation and the City Police in respect of cyber threats. In particular it considers progress in respect of;

- Policy – a fully embedded Information Security policy, covering cyber security risks is in place at the City Police, whilst a comprehensive Information Security policy, likewise covering cyber security risks has been developed and is pending approval at the City Corporation. Employees have received adequate training to mitigate against the human risks to cyber security, through a programme of mandatory information security training.
- Department for Communities and Local Government (DCLG) guidance on cyber resilience - fully embedded at the City Police and comprehensively integrated at the City Corporation, with work in place to strengthen resilience in a small number of areas.
- Internal Assurance – internal assurance is to be gained by regularly re-assessing the extent to which cyber risks are reviewed as part of the Internal Audit work programme. Contracted IT service providers are required to meet specified security standards as defined by the City Corporation in business partnership contracts; this includes the requirement from Agilisys to ensure compliance with the PSN & PSNP requirements.

- External Assurance - the PSN (Public Secure Network) and PSNP (Public Secure Network - Police) external review process provides an appropriate level of assurance that the City Corporation and City Police networks are operating in a secure manner. Both the City Corporation and City Police are fully compliant with the secure network requirements and hold accreditation from the Cabinet Office and Home Office respectively. Baker Tilley will be reviewing the City Corporation and City Police response to the DCLG guidance on cyber resilience in order to provide additional assurance.

Members are asked to:

- Note the report.

## **Background**

1. Cyber security and associated risks are a growing issue for organisations, both within the public and private sectors; the City of London Corporation and the City of London Police are not exempt from these risks, and it is essential that the risks are understood, and robust controls are established to secure the City Corporation and City of London Police from these threats. The Committee received a report in April setting out the cyber fraud risks facing the City Corporation and the City Police. The report summarised the potential vulnerabilities, possible audit activity and action being taken by management to minimise the threat of successful fraud. Following on from the June Committee, the Internal Audit team was asked to establish what the current position is in relation to the measures in place to mitigate cyber threats.

## **Current Position**

2. The Internal Audit team has conducted an initial review of cyber security requirements for both the City of London Corporation and the City of London Police and their position in relation to the key control framework requirements for cyber security, including Department for Communities and Local Government Guidance (DCLG), Public Secure Network (PSN & PSNP) requirements and Information Security policies, which incorporate cyber security. Findings have identified that the cyber security requirements for the City of London Police are far greater than those for the City of London Corporation, however it is essential that cyber risks for both organisations are managed effectively in order to mitigate the overall risks of attack.

### City of London Police Information Security Policy

3. The City of London Police Information Security Policy outlines how the City Police safeguard and protect information assets from potential security threats with the following:
  - Information Security Procedures Manual
  - Acceptable Use Policy
  - Forensics Readiness Policy



4. The Information Security Procedures Manual covers information security threats, internal and external produced in line with regulatory requirements covering:
- Information risk management regime
  - Secure configuration
  - Network security
  - Managing user privileges
  - User education and awareness
  - Incident management
  - Malware prevention
  - Monitoring
  - Removable media controls
  - Home and mobile working

#### City of London Corporation Information Security Policy

5. The City Corporation's Information Security policy is currently in draft format and is pending approval by senior management. The policy covers information security threats, internal and external, produced in line with ISO 27002:2013 standards and guidance from the Information Commissioner, local Government, the Cabinet Office and other regulatory bodies. The policy includes:
- User authentication
  - Device access and allocation
  - Remote access
  - Internet and social media
  - System access and use
  - Email access and use
  - Information sharing
6. The City Police's Information Security policy provides an established and developed response to cyber security risks, in line with the significant security requirements expected of a Police force. The City Corporation's draft Information Security policy represents a proportionate approach to cyber security risks affecting local government organisations.
7. The City Corporation and City of London Police have taken reasonable steps to ensure that employee's receive appropriate training to mitigate against the human risks to cyber security, through a programme of mandatory information security training.

## **Department for Communities and Local Government (DCLG) Guidance – Understanding Local Cyber Resilience, 10 steps to cyber security**

8. We have benchmarked the cyber security response for the City Corporation and the City Police against DCLG guidance – Understanding Local Cyber Resilience, 10 steps to cyber security, issued in March 2015 (Appendix 1), which covers:
- Information Risk Management Regime
  - Secure Configuration
  - Network Security
  - Managing User Privileges
  - User Education and Awareness
  - Incident Management
  - Malware Prevention
  - Monitoring
  - Removable Media Controls
  - Home & Mobile Working
9. The DCLG cyber security measures are fully embedded at the City Police, as would be expected for an organisation requiring significant security standards. The City Corporation, with a lower level of cyber risk, has measures in place in all key requirements, however a small number of additional measures have been identified where controls can be strengthened, these are;
- a) Finalise approval of the City Corporation's Information Security policy, which incorporates cyber security.
  - b) Strengthen network access controls as an additional security feature.
  - c) Ensure consistency in the application of processes for joiners, movers and leavers.
  - d) Consider creating a central repository for system logs, gathering network data and enabling analysis and interrogation of suspect cyber activity.

### **External and Internal Assurance**

10. The Public Services Network (PSN) is a UK Government programme to unify the provision of network infrastructure across the United Kingdom public sector into an interconnected "network of networks" to increase efficiency and reduce overall public expenditure.
11. PSN compliance requirements are designed to protect the organisations network. The Police Service Network in Policing (PSNP) scheme provides Police forces with improved security and accreditation to Home Office standards. Similarly, the compliance requirements for local Government, although not as extensive, also provide local Government organisations with improved security processes and procedures as set out by the PSN team, within the Cabinet Office.

12. The City Corporation (PSN) and City Police (PSNP) are compliant with the secure network requirements, and hold accreditation from the Cabinet Office and Home Office respectively. The PSN and PSNP external review process provides an appropriate level of assurance that the City Corporation and City of London Police networks are operating in a secure manner
13. PSN compliance is not the only way to deliver security across the organisations. Directing resources towards simply meeting PSN requirements is no substitute for engaging in ongoing risk assessment, management and mitigation across both organisations.
14. Both the City Corporation and City of London Police take reasonable steps, in addition to PSN requirements to monitor the networks for cyber threats.
15. A Police Service Risk Management Organisation annual report is produced and submitted by the City of London Police to the Home Office, in respect of cyber security risks. This includes an information assurance maturity model assessment performed against the following criteria with 1-5 rating
  - Leadership & Governance
  - Training Education & Awareness
  - Information Risk Management
  - Assured Information Sharing
  - Compliance
16. An inspection by the Information Commissioner considered the City of London Police to be exemplary in the cyber security work undertaken, and recommended that the City Police be an example for other forces to follow.
17. The City of London Corporation external penetration testing, conducted in January 2015, and detailed in the non-public report to this Committee in April 2015, provided additional assurance on the strength of the security controls adopted by the City Corporation in response to cyber threats.
18. The Internal Audit IT programme of work has been designed to review cyber associated risks, as set out in the cyber risks paper presented to this Committee on 28 April 2015. Internal Audit will continue to regularly review the programme of IT audit work to ensure that it accurately reflects the cyber risks affecting the City Corporation and the City Police.
19. Baker Tilly's IT Audit team will provide a further external check of conformity with the DCLG guidance for local cyber resilience and advise on the accuracy of policy and procedures covering cyber security.
20. Contracted IT service providers are required to meet specified security standards as defined by the City Corporation in business partnership contracts; this includes the requirement from Agilisys to ensure compliance with the PSN & PSNP requirements.

## Conclusion

21 The City of London Police has developed and maintains a robust response to cyber related threats. The City Police response to cyber threats is in line with the expectations for an organisation holding sensitive and confidential personal data. The programme of annual external reviews for the City Police provides a strong level of assurance that cyber threats are being managed effectively.

22 The City of London Corporation has a proportionate response to cyber threats, it has achieved PSN compliance and is currently developing cyber related policy and procedure through the information security roadmap, which will provide the City Corporation with additional confidence that the threats posed can be managed adequately.

## Appendices

- Appendix 1 – 10 Steps to Cyber Security
- Appendix 2 – DCLG Paper: Understanding Local Cyber Resilience (March 2015)

### Chris Harris

Head of Internal Audit

T: 07800 513179

E: [chris.harris@cityoflondon.gov.uk](mailto:chris.harris@cityoflondon.gov.uk)

## Appendix 1 – DCLG 10 Steps to Cyber Security

### Cyber Security Measure

**Information Risk Management Regime** - Assess the risks to your organisation's information assets with the same vigour as you would for legal, regulatory, financial or operational risk. To achieve this, embed an Information Risk Management Regime across your organisation, supported by the Board, senior managers and an empowered information assurance (IA) structure. Consider communicating your risk management policy across your organisation to ensure that employees, contractors and suppliers are aware of your organisation's risk management boundaries.

**Secure configuration** - Introduce corporate policies and processes to develop secure baseline builds, and manage the configuration and use of your ICT systems. Remove or disable unnecessary functionality from ITC systems, and keep them patched against known vulnerabilities. Failing to do this will expose your business to threats and vulnerabilities, and increase risk to the confidentiality, integrity and availability of systems and information.

**Network security** - Connecting to untrusted networks (such as the Internet) can expose your organisation to cyber-attacks. Follow recognised network design principles when configuring perimeter and internal network segments, and ensure all network devices are configured to the secure baseline build. Filter all traffic at the network perimeter so that only traffic required to support your business is allowed, and monitor traffic for unusual or malicious incoming and outgoing activity that could indicate an attack (or attempted attack).

**Managing user privileges** - All users of your ICT systems should only be provided with the user privileges that they need to do their job. Control the number of privileged accounts for roles such as system or database administrators, and ensure this type of account is not used for high risk or day-to-day user activities. Monitor user activity, particularly all access to sensitive information and privileged account actions (such as creating new user accounts, changes to user passwords and deletion of accounts and audit logs).

**User education and awareness** - Produce user security policies that describe acceptable and secure use of your organisation's ICT systems. These should be formally acknowledged in employment terms and conditions. All users should receive regular training on the cyber risks they face as employees and individuals. Security related roles (such as system administrators, incident management team members and forensic investigators) will require specialist training.

**Incident management** - Establish an incident response and disaster recovery capability that addresses the full range of incidents that can occur. All incident management plans (including disaster recovery and business continuity) should be regularly tested. Your incident response team may need specialist training across a range of technical and non-technical areas. Report online crimes to the relevant law enforcement agency to help the UK build a clear view of the national threat and deliver an appropriate response.

**Malware prevention** - Produce policies that directly address the business processes (such as email, web browsing, removable media and personally owned devices) that are vulnerable to malware. Scan for malware across your organisation and protect all host and client machines with antivirus solutions that will actively scan for malware. All information supplied to or from your organisation should be scanned for malicious content.

**Monitoring** - Establish a monitoring strategy and develop supporting policies, taking into account previous security incidents and attacks, and your organisation's incident management policies. Continuously monitor inbound and outbound network traffic to identify unusual activity or trends that could indicate attacks and the compromise of data. Monitor all ICT systems using Network and Host Intrusion Detection Systems (NIDS/HIDS) and Prevention Systems (NIPS/HIDS).

**Removable media controls** - Produce removable media policies that control the use of removable media for the import and export of information. Where the use of removable media is unavoidable, limit the types of media that can be used together with the users, systems, and types of information that can be transferred. Scan all media for malware using a standalone media scanner before any data is imported into your organisation's system.

**Home and mobile working** - Assess the risks to all types of mobile working (including remote working where the device connects to the corporate network infrastructure) and develop appropriate security policies. Train mobile users on the secure use of their mobile devices for locations they will be working from. Apply the secure baseline build to all types of mobile device used. Protect data-at-rest using encryption (if the device supports it) and protect data-in-transit using an appropriately configured Virtual Private Network (VPN).



Department for  
Communities and  
Local Government

# Understanding Local Cyber Resilience

A guide for local government on cyber threats and how to  
mitigate them



© Crown copyright, 2015

*Copyright in the typographical arrangement rests with the Crown.*

You may re-use this information (not including logos) free of charge in any format or medium, under the terms of the Open Government Licence. To view this licence, <http://www.nationalarchives.gov.uk/doc/open-government-licence/version/3/> or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: [psi@nationalarchives.gsi.gov.uk](mailto:psi@nationalarchives.gsi.gov.uk).

This document/publication is also available on our website at [www.gov.uk/dclg](http://www.gov.uk/dclg)

If you have any enquiries regarding this document/publication, complete the form at <http://forms.communities.gov.uk/> or write to us at:

Department for Communities and Local Government  
Fry Building  
2 Marsham Street  
London  
SW1P 4DF  
Telephone: 030 3444 0000

For all our latest news and updates follow us on Twitter: <https://twitter.com/CommunitiesUK>

March 2015

ISBN: 978-1-4098-4619-2



# Contents

<b>Introduction</b>	<b>4</b>
Cybercrime	5
Hactivism	6
Insiders	7
Physical threats	8
Terrorists	8
Espionage	9
What you can do and who can help	10
Conclusion	14

# Introduction

This paper, commissioned by the Department for Communities and Local Government and prepared in collaboration with the Cabinet Office, outlines the key cyber resilience threat to Local Government. This is a persistent threat that, if left unchecked, could disrupt the day-to-day operations of councils, the delivery of local public services and ultimately has the potential to compromise national security.

Technical advances create opportunities for greater efficiency and effectiveness. These include more engaging and efficient digital services, new ways to work remotely and to store and transfer data, such as mobile devices and cloud services. However, these also present more opportunities for attackers. The networks and public-facing websites of every local authority are threatened. On average, 33,000 malicious emails are blocked from accessing public sector systems every month and this is just one of the many different types of attack government and wider public service systems must defend against. The scale of the targeting, coupled with the difficulty of monitoring all possible attack methods, means some attacks will get through but our collective responsibility is to both reduce the likelihood and the impact of such a threat succeeding. Foreign states, criminals, hacktivists, insiders and terrorists all pose different kinds of threat. They may try to compromising public sector networks to meet various objectives that include:

- Stealing sensitive information to gain an economic, diplomatic or military advantage over the UK
- Financial gain
- Attracting publicity for a political cause
- Embarrassing central and local government
- Controlling computer infrastructure to support other nefarious activity
- Disrupting or destroying computer infrastructure

Whilst the level of threat will vary across local authorities they all possess information or infrastructure of interest to malicious cyber attackers. Council employees can also be targets for criminal activity. Across the country local government IT departments are working hard to reduce these threats every day and the support of senior officers and councillors is vital to ensuring the continued focus and profile of this work. This guide is intended to help the non-technical reader understand the threats and what can be done to reduce their organisations' vulnerability to security incidents and cyber-attacks.

# Cybercrime

Cybercriminals' principal goal is to monetise their attacks. The most common form of cyber-attack against public bodies is the use of false or stolen customer credentials to commit fraud. The uptake in online services means this form of crime can now be done on a much larger scale and foreign nationals as well as onshore criminals can defraud local authorities from outside the UK. Cybercriminals also seek to steal data from government networks that has a value on the black market, such as financial information or data that can be used for ID theft. Several types of malware have been specifically designed by cybercriminals to exploit e-banking details or log-in information. These include Shylock, Gameover Zeus and Citadel. Such malware is sometimes found on public sector networks, but financial and commercial organisations are more likely to be targeted.

Cybercriminals often want to control computer infrastructure and use it as a platform for carrying out other activity such as sending spam and phishing emails. Government networks are an attractive target. These groups also launch ransom attacks, locking victims out of their data and only providing the key once money is paid. Although the victims are usually members of the public and sometimes small organisations, the criminals often purport to come from a public agency leading to the potential for reputational damage.

A recent E-Government Bulletin survey highlighted the concerns amongst Councils of being exposed to risks of losing website traffic, and even blackmail, through 'cybersquatting' of internet domain names. Cyber squatters use these domains to draw traffic away from council sites to their own commercial information services, and perhaps to publish material attacking the council or to imply an endorsement which does not exist.

Despite the continued success of National Crime Agency (NCA) and FBI operations in the USA, cybercriminals adapt their methods and tools to counter law enforcement action. It therefore takes a sustained campaign to keep cyber-security standards up to date. Removing malware from a network is a complex and time-consuming task that would have a significant impact on the running of an organisation, especially if a network needs to be shut down – so prevention is better than cure. Public bodies that fail to secure personal data will be investigated by the Information Commissioner and can expect a fine if found negligent.

# Hacktivism

Hacktivismists crave publicity. For them, success is for example causing embarrassment or annoyance to the owners of high-profile websites and social media platforms that they deface or take offline. When targeted against local government websites and networks, these attacks can cause reputational damage locally and to the UK at home and abroad. Hacktivismist groups have successfully used distributed denial of service (DDoS) attacks to disrupt the websites of UK local authorities. A DDoS is when a system, service or network is burdened to such an extent by an electronic attack that it becomes unavailable. If targeted at online public services (such as UK visas, Universal Credit, Council Tax payments) this kind of attack would cause financial, as well as reputational harm.

In July 2014 a Council member's Twitter account was hacked. A hacktivismist group claimed responsibility and posted political statements. The council involved shut down its entire email system while it investigated.

A May 2014 global survey commissioned by BT showed, on average, organisations take 12 hours to recover fully from an especially powerful DDoS attack. If online services are regularly disrupted by cyber-attacks this could lead to the erosion of public confidence in using such services. Lone hacktivismists can pursue their own personal agenda. They do not require detailed technical know-how to achieve their goal. There are many commercially available hacking tools which have easy, step-by-step guides providing motivated but low-skilled individuals with the opportunity to gain illegitimate access to networks. The social media accounts (Facebook, Twitter and LinkedIn) of local authorities and individuals can be hijacked and misleading information posted.

The website of a major unitary authority in the Midlands was taken down by online attackers in 2012. As a result outside browsers wishing to check on services like council tax details, report service issues, pot holes or find out about library times or council committee meetings were unable to do so for up to 48 hours after the initial attack.

# Insiders

An insider is someone who exploits, or intends to exploit, their legitimate access to an organisation's assets for unauthorised purposes. Such activity can include:

Unauthorised disclosure of sensitive information

Facilitation of third party access to an organisation's assets

Physical sabotage

Electronic or IT sabotage

Not all insiders deliberately set out to betray their organisation. An unwitting insider may compromise their organisation through poor judgement or due to a lack of understanding of security procedures. The insider threat is not new, but the environment in which insiders operate has changed significantly. Technological advances have created broader opportunities for staff at all levels to access information. These advances have also made it easier for insiders to collate, remove and circulate vast volumes of sensitive data and local authorities are at risk. Although the number of potential insiders within an organisation is proportionately very small, the potential impact on government and wider public sector is significant.

A clerk at a Magistrates Court was jailed for seven years in 2011 after taking bribes for using privileged access to court systems to help offenders avoid prosecution.

A council worker based in a unitary authority in North East England had been working with information held on a USB stick while using a laptop that was connected to the council's networked computer system. When logging off the system and leaving the office for the day, the user forgot to remove the USB stick. When the employee realised the mistake and tried to retrieve the USB stick, it was gone. As a result the council was subject to a significant fine from the Information Commissioner for the data loss.

# Physical threats

The increasing reliance on digital services brings with it an increased vulnerability in the event of a fire, flood, power cut or other disaster natural or otherwise that impact upon local government IT systems. Authorities take a range of approaches to mitigating threats in this area ranging from accepting the risk (for low impact services), to ensuring information is backed up off site (for medium impact services), having plans in place to recover services in an alternative location (for high impact services), to full resilience across more than one location (for very high impact services). Many local authorities are starting to share services and locations to provide resilience in a cost effective way.

In 2013 a council in the north of England suffered a second fire in a data centre in the space of 24 months so took the decision to invest in a fully resilient solution that now enables them to recover their services in a very short space of time and alternative location in the event of a fire, flood or terrorist event.

# Terrorists

Some terrorist groups demonstrate intent to conduct cyber-attacks, but fortunately have limited technical capability. Terrorist groups could acquire improved capability in a number of ways, namely through the sharing of expertise in online forums providing a significant opportunity for terrorists to escalate their capability.

Terrorist propaganda hacks occur across local public sector on an ad hoc basis such as the case of a town council in the south east that was hacked; viewers accessing the councils' web pages were confronted with the image of a hooded combat figure dressed in black.

So whilst many hacktivist groups do not pose a significant threat to the UK, they do possess skills and capabilities which are desired by some terrorist groups. Terrorists may learn from large-scale data deletion attacks – such as the attack against the Saudi Arabian national oil company, Saudi Aramco, in which data on 30,000 computers was lost – and aspire to have the same impact in the UK.

# Espionage

Several of the most sophisticated and hostile foreign intelligence agencies target UK government and public sector networks to steal sensitive information. This could ultimately disadvantage the UK in diplomatic or trade negotiations, or militarily. In a recent case a hostile, state-sponsored group gained access to a system administrator account on the Government Secure Intranet. Fortunately this attack was discovered early and dealt with to mitigate any damage but it and the example below from Canada illustrates the potential threat from cyber-espionage in this way to both central and local government.

Hackers, believed to be linked to a foreign state, gained control of a number of Canadian Government computers belonging to senior officials. The hackers, then posing as the officials, sent emails to administrators, conning them into providing key passwords that unlocked access to government networks. At the same time, the hackers sent other staff seemingly innocuous memos as attachments. The moment a recipient opened the attachment, malware infected the network. The malware looked for specific kinds of classified government information and sent it back to the hackers over the internet. Once the compromise was detected, access to the internet was shut down for thousands of public servants.

The internet's global nature enables hostile foreign intelligence agencies to conduct espionage on an ever-increasing scale with the added benefit of using deniable infrastructure to keep their activity hidden. This technical infrastructure allows sophisticated state actors to obfuscate their location, making Government networks an attractive target for state cyber programmes. Employees are also a target for hostile foreign intelligence agencies.

# What you can do and who can help

As well as localised threats such as flood or fire the global nature of the internet and its potential for deniability makes it fertile ground for all kinds of cyber-attack. The UK, as one of the world's most internet-dependent nations, is particularly vulnerable. Attackers can use multiple methods to steal your organisation's information or disrupt its systems and it is not currently possible to keep out all the attacks, all the time. Inevitably disasters occur and some attackers will get through, which makes a robust cyber incident management plan essential for all public sector organisations. Advice on protective security is available on the websites of Centre for the Protection of the National Infrastructure ([www.cpni.gov.uk](http://www.cpni.gov.uk)) and Communications-Electronics Security Group ([www.cesg.gov.uk](http://www.cesg.gov.uk)).

## Adopt the 10 Steps to Cyber Security approach

A good starting point is adopting the basic cyber-security measures, set out in CESG's the [10 Steps to Cyber-security](#), is highly effective at preventing most attacks. A more detailed guide around how to brief board-level corporate and business decision making can be found at <http://www.cpni.gov.uk/highlights/cyber-advice-businesses/>

- **Information Risk Management Regime** - Assess the risks to your organisation's information assets with the same vigour as you would for legal, regulatory, financial or operational risk. To achieve this, embed an Information Risk Management Regime across your organisation, supported by the Board, senior managers and an empowered information assurance (IA) structure. Consider communicating your risk management policy across your organisation to ensure that employees, contractors and suppliers are aware of your organisation's risk management boundaries.
- **Secure configuration** - Introduce corporate policies and processes to develop secure baseline builds, and manage the configuration and use of your ICT systems. Remove or disable unnecessary functionality from ICT systems, and keep them patched against known vulnerabilities. Failing to do this will expose your business to threats and vulnerabilities, and increase risk to the confidentiality, integrity and availability of systems and information.
- **Network security** - Connecting to untrusted networks (such as the Internet) can expose your organisation to cyber-attacks. Follow recognised network design principles when configuring perimeter and internal network segments, and ensure all network devices are configured to the secure baseline build.



Filter all traffic at the network perimeter so that only traffic required to support your business is allowed, and monitor traffic for unusual or malicious incoming and outgoing activity that could indicate an attack (or attempted attack).

- **Managing user privileges** - All users of your ICT systems should only be provided with the user privileges that they need to do their job. Control the number of privileged accounts for roles such as system or database administrators, and ensure this type of account is not used for high risk or day-to-day user activities. Monitor user activity, particularly all access to sensitive information and privileged account actions (such as creating new user accounts, changes to user passwords and deletion of accounts and audit logs).
- **User education and awareness** - Produce user security policies that describe acceptable and secure use of your organisation's ICT systems. These should be formally acknowledged in employment terms and conditions. All users should receive regular training on the cyber risks they face as employees and individuals. Security related roles (such as system administrators, incident management team members and forensic investigators) will require specialist training.
- **Incident management** - Establish an incident response and disaster recovery capability that addresses the full range of incidents that can occur. All incident management plans (including disaster recovery and business continuity) should be regularly tested. Your incident response team may need specialist training across a range of technical and non-technical areas. Report online crimes to the relevant law enforcement agency to help the UK build a clear view of the national threat and deliver an appropriate response.
- **Malware prevention** - Produce policies that directly address the business processes (such as email, web browsing, removable media and personally owned devices) that are vulnerable to malware. Scan for malware across your organisation and protect all host and client machines with antivirus solutions that will actively scan for malware. All information supplied to or from your organisation should be scanned for malicious content.
- **Monitoring** - Establish a monitoring strategy and develop supporting policies, taking into account previous security incidents and attacks, and your organisation's incident management policies. Continuously monitor inbound and outbound network traffic to identify unusual activity or trends that could indicate attacks and the compromise of data. Monitor all ICT systems using Network and Host Intrusion Detection Systems (NIDS/HIDS) and Prevention Systems (NIPS/HIDS).
- **Removable media controls** - Produce removable media policies that control the use of removable media for the import and export of information. Where

the use of removable media is unavoidable, limit the types of media that can be used together with the users, systems, and types of information that can be transferred. Scan all media for malware using a standalone media scanner before any data is imported into your organisation's system.

- **Home and mobile working** - Assess the risks to all types of mobile working (including remote working where the device connects to the corporate network infrastructure) and develop appropriate security policies. Train mobile users on the secure use of their mobile devices for locations they will be working from. Apply the secure baseline build to all types of mobile device used. Protect data-at-rest using encryption (if the device supports it) and protect data-in-transit using an appropriately configured Virtual Private Network (VPN).

## Join the Cyber-security Information Sharing Partnership (CiSP)

In addition to these resources, the Cyber-security Information Sharing Partnership (CiSP) [www.cert.gov.uk/cisp](http://www.cert.gov.uk/cisp) (part of and Computer Emergency Response Team CERT-UK), allows members from across sectors and organisations to exchange cyber threat information in real time, on a secure and dynamic environment, whilst operating within a framework that protects the confidentiality of shared information. It is a joint industry/government initiative to share cyber threat and vulnerability information in order to increase overall situational awareness of the cyber threat and therefore reduce the impact on the UK. CiSP members benefit from:

Engagement with industry and government counterparts in a secure environment  
Early warning of cyber threats  
Ability to learn from experiences, mistakes, successes of other users and seek advice  
An improved ability to protect their corporate business network

CiSP is free to join and a dedicated forum for local authorities exists on the CiSP platform, this is specifically to enhance the ability of organisations to share sensitive information in a safe and trusted environment. An increasing number of local authorities are joining CiSP to help become better equipped to deal with such new and emerging threats. Working with others in this way is enabling them to fully utilise the benefits of working at a network defending level - to secure local authorities against the online threats to both their operations and the data held in their care.

The ability of CISP members to deal with the recent Heartbleed vulnerability incident illustrated of the benefit of being a member; a dedicated group was established allowing members to easily access the latest information and

mitigation advice, including privileged information that had a direct impact on members' ability to update their firewalls in a timely fashion.

It is important to remember however, that should a local authority fall victim to a cyber-attack it should report the incident to [GovCertUK](#) in the first instance.

## **To find out more**

The application process to join CiSP is straightforward with details available [at \*\*www.cert.gov.uk/cisp\*\*](#). In addition for further details about the CiSP please contact CERT-UK at <https://www.cert.gov.uk/contact-us/contact-form/>

# Conclusion

This guide is intended to provide the basis for non-technical senior managers and leaders to gain a better understanding of the potential threats from cyber-attack and how local authorities can reduce their vulnerability to threats. Getting cyber resilience right has never been more important as public services continue to modernise and improve our ways of working and as we deliver more and more services online.

Ultimately being cyber resilient is about having the right resilience, appropriately tailored to take proper account of the very wide range of different activities councils undertake, the assets they handle and environments they work in. Focus in this area will help ensure that local authorities can gain and develop the public's trust that they will handle their information properly and protect the public, commercial and financial interests they are responsible for on behalf of their local communities.



This page is intentionally left blank

<b>Committee(s):</b>	<b>Date(s):</b>
Audit and Risk Management Committee	
<b>Subject:</b> HMIC Inspection Update	<b>Public</b>
<b>Report of:</b> Commissioner, City of London of Police	<b>For Information</b>

## Summary

This report provides Members with an overview of the City of London Police response to Her Majesty's Inspectorate of Constabulary's (HMIC) continuing programme of inspections and published reports. It also provides assurance that the recommendations from reports are being addressed by the Force.

During the reporting period (September 2014 – September 2015) HMIC has published ten reports (three being joint reports with other agencies) and one assessment letter:

- Strategic Policing Requirement (Force-specific)
- Undercover Policing (National report)
- PEEL Interim Assessment (incorporating Crime Inspection) (Force – specific)
- Police Integrity and Corruption (Force-specific)
- Integrity Matters (National report)
- Joint Inspection of the investigation and prosecution of fatal road traffic collisions (National report)
- Welfare of vulnerable people in police custody (National Report)
- Stop and search powers 2: are police using them effectively and fairly (National report)
- Joint Review of Disability Hate Crime follow-up (National report)
- Joint Inspection of the Provision of Charging Decisions (National Report) ; and
- Phase 1 assessment of preparedness to protect victims of so-called Honour Based Violence (HBV), Forced Marriage (FM) and Female Genital Mutilation (FGM). (Force-specific assessment letter).

The assessment letter is City of London specific and is based on a desktop inspection (i.e. HMIC did not visit the Force to interview staff or check systems).

This report is supported by Appendix A which provides details of progress against all outstanding HMIC recommendations. The Appendix only reproduces all the recommendations from the most recent reports (i.e. those reported to the last Police Performance and Resource Management Sub Committee on 30<sup>th</sup> June 2015) together with all outstanding recommendations from earlier reports.

All reports and progress against recommendations are reported in detail quarterly to the Police Performance and Resource Management Sub Committee for scrutiny and oversight.

### **Recommendation**

Members are asked to receive this report and note its contents.

## **Main Report**

1. This report provides Members with an overview of the City of London Police response to Her Majesty's Inspectorate of Constabulary's (HMIC) continuing programme of inspections and published reports. During the reporting period, (June 2014 – June 2015) HMIC, either alone or with other agencies, has published ten reports.
2. Additionally, on 15<sup>th</sup> May 2015, HMIC wrote to the Force with its draft assessment of the Force's preparedness to protect victims of Honour Based Violence (HBV) following a desk top inspection of all 43 police forces.
3. Appendix A to this report provides an overview of progress against all outstanding HMIC recommendations. All reports and progress against recommendations are reported in detail quarterly to the Police Performance and Resource Management Sub Committee for scrutiny and oversight

### **Strategic Policing Requirement (Force specific report)**

4. This report was one of eighteen force-specific reports. It was a supplementary report to the national report that was previously reported to the Police Performance and Resource Management Sub Committee (Pol 41-14 refers).
5. HMIC found that the Force has the necessary capacity, capability, consistency and connectivity to fulfil its obligations across the five areas of the Strategic Policing Requirement (terrorism, civil emergencies, public order, serious organised crime and large scale cyber attacks). Some comments were made regarding improvements that could be made with respect to cyber crime (which were addressed by the Force's Cyber Crime Strategy), however, the report did not make any formal recommendations for improvement.

### **Undercover Policing (National Report)**

6. The report, 'An inspection of undercover policing in England and Wales', examined the effectiveness of the arrangements in place in all 43 police forces to carry out, manage and scrutinise undercover operations.
7. The report's principal findings were that undercover officers are dedicated individuals that deliver their roles professionally. The essential need for undercover policing was also recognised.



8. The report made a total of 49 recommendations across policies, systems, training and leadership of undercover operations which HMIC felt were necessary to address the inconsistencies and shortcomings identified by the inspection, of these 15 were assessed as being specific to the Force with the majority applied to national lead organisations within this field.

### **Police Effectiveness, Efficiency and Legitimacy (PEEL) Interim Assessment (Force specific)**

9. The PEEL assessment provided a broad assessment of policing over the three pillars of effectiveness, efficiency and legitimacy. Every inspection conducted by HMIC during 2014 in some way contributed to the evidence for the gradings received.
10. HMIC labelled the first assessment as interim because it was based on an incomplete set of inspections. However, HMIC felt that there was sufficient evidence to publish the interim assessment.
11. The website presents a high level narrative judgement for each pillar together with an overall assessment of the Force based on the HMI's professional judgement. Readers are directed to individual inspection reports for detailed findings.
12. The Force received an overall assessment of GOOD. HMIC stated the available evidence indicated that:
  - in terms of its effectiveness, the force is good at reducing crime and preventing offending, good at investigating offending and good at tackling anti-social behaviour;
  - the efficiency with which the force carries out its responsibilities is good; and
  - the Force is acting to achieve fairness and legitimacy in most of the practices that were examined this year.
13. The PEEL assessment did not make any recommendations.

### **Police Integrity and Corruption (Force-specific report)**

14. The *Police Integrity and Corruption* report was the third in a series that began in 2011 when HMIC was formally commissioned by the Home Secretary to consider instances of undue influence, inappropriate contractual arrangements and other abuses of power in police relationships with the media and other parties.
15. Overall, HMIC found that the Force had made good progress on the 3 areas for improvement identified in the previous report and that officers understood values and professional behaviour across the organisation. They found the Commissioner and his chief officer team set high standards in terms of conduct and behaviour and other senior leaders understand their responsibilities to maintain and promote these standards throughout the

Force. They also commented positively on the Force's mandatory e-learning training package ensuring staff had read and understood the Code of Ethics.

16. Whilst HMIC found that the Force actively and effectively identifies and manages threat, risk and harm from corruption, taking all reasonable steps to ensure that organised crime investigations are not compromised, they did feel there were insufficient resources within the counter-corruption unit (CCU) to deal effectively with the flow of intelligence.

17. HMIC only recommended 4 areas for improvement, all of which have been implemented.

### **Integrity Matters: National Report on Police Integrity and Corruption**

18. The report presented a comprehensive assessment of:

- Discovering, investigating and tackling wrongdoing;
- Misconduct and corruption;
- Revisiting police relationships;
- Role of leadership in creating ethical culture;
- Policies and practices to promote integrity;
- Anti-corruption systems and processes;
- Capacity and capability of professional standards departments and anti-corruption units.

19. HMIC's principal findings nationally were:

- The arrangements that forces have in place are in appreciably better shape than when the first reviews into this area were conducted in 2011 and 2012.
- Chief officers are taking seriously issues of police integrity and making tangible progress in creating an ethical culture (chiefly through embedding the Police Code of Ethics).
- Forces are using a wide range of structures and resourcing models for the professional standards and anticorruption departments; they did not consider any one model better than another, recognising that they often reflected local circumstances.

20. The report made 14 recommendations, all of which have been addressed by the Force.

### **Joint Inspection of the investigation and prosecution of fatal road traffic incidents (National report)**

21. This report followed a joint thematic inspection by HMIC and the Crown Prosecution Service. Only six forces and CPS areas were inspected, however, all police forces provided data submissions that informed the final report.

22. The report made 4 recommendations for the police service, all of which the Force was already complying with.

### **The welfare of vulnerable people in police custody (National report)**

23. This report followed a thematic inspection on the welfare of vulnerable people in police custody, including but not limited to those with mental health issues, those from black and minority ethnic backgrounds and children, Only six forces were inspected although all 43 forces provided data submissions to inform the final findings.
24. HMIC made 18 detailed recommendations as a result of this inspection. Of those recommendations, 7 are for police forces to consider and progress, the remainder being recommendations aimed at the Home Office, College of Policing and other agencies.
25. The recommendations are included in Appendix A together with details of work that is progressing to comply with them.

### **Stop and Search Powers 2: Are the Police using them effectively and fairly (National report)**

26. This report assessed progress made nationally since the original 2013 HMIC Stop and Search inspection. All 43 forces were contacted and asked to supply data. Only 6 forces were actually visited by HMIC, City of London was not one of those forces.
27. The report made 11 recommendations. Of those, only 3 are for forces to address directly, the remainder are directed at the Home Office, the National Police Chiefs' Council and the College of Policing either individually or jointly. All the recommendations are included in Appendix A to this report.

### **Joint review of Disability Hate Crime follow up. (National report)**

28. This joint follow up review considered how the police, Crown Prosecution Service and national probation service providers have responded to the 7 recommendations made by the Criminal Justice Joint Inspection (CJJI) review of disability hate crime published in March 2013. 6 police forces were inspected as part of the review; the City of London Police was not one of them.
29. The 2013 review highlighted the need for the 3 agencies to take appropriate steps to ensure that the public and those working in the criminal justice system understood disability hate crime. Of the 7 recommendations made as a result of the 2013 review, 3 were joint actions for all three agencies (at national association level), 1 was directed solely at the police service, 2 were for the CPS and 1 was for the national probation service providers. Only the recommendation relevant to the police is detailed below.

- Forces should review the methods by which information is received from the public to ensure that every opportunity is being taken to identify victims of disability hate crime. The CJI found no evidence that any of the 6 forces inspected had conducted such a review and none routinely scrutinised the means by which victims of disability hate crime chose to report crimes. There have been no reports of disability hate crime made in the City of London since 2011/12 (when there were 2). However, the Force has implemented various measures (including training and awareness campaigns for officers and the public) that will assist in identifying victims of disability hate crime.

### **Joint Inspection of the Provision of Charging Decisions (National report)**

30. The Provision of Charging Decisions report details the findings of a joint inspection carried out by Her Majesty's Crown Prosecution Service Inspectorate (HMCPPI) and HMIC that scrutinised how well the police and CPS ensure quality charging decisions are made. The inspection also looked at progress made since the last full inspection of this area, which was in 2008.
31. The inspectors visited 6 police forces and their aligned CPS areas<sup>1</sup> and examined 650 police and CPS charged cases. The City of London Police was not involved in the inspection.
32. The report made 10 recommendations, reproduced in full in Appendix A. Only 3 recommendations relate to the police service.

### **Phase 1 Honour Based Violence, Forced Marriage and Female Genital Mutilation Inspection (Force specific)**

33. On the 13<sup>th</sup> May, the HMIC wrote to the Force with a draft assessment of the Phase 1 results from a current series of inspections examining forces responses to Honour Based Violence (HBV), Forced Marriage (FM) and Female Genital Mutilation. The Force was not visited by HMIC, relying instead on a standardised response to a request for data. The assessment was in the form of a letter and no recommendations for improvement were made. However, because HMIC have used a strict, standardised methodology to form the overall assessment, the City of London Police was assessed as not yet prepared across all areas to protect people from harm from HBV. This assessment was challenged by the Force, however, that challenge was not successful.
34. The Commissioner wrote to HMIC to request the assessment is reconsidered as it presents a misleading picture of the actual situation. HMIC responded (verbally) that to maintain a consistent approach to assessments nationally, they did not intend to alter their assessment on this occasion.

---

<sup>1</sup> Cheshire, Merseyside (CPS Mersey-Cheshire); Devon and Cornwall, Gloucestershire (CPS South West); MPS (CPS London); and South Wales (CPS Cymru-Wales)

35. Phase 2 of the inspection will be on risk based basis and HMIC has already confirmed that the City of London Police will not be inspected.

## **Appendix**

36. Appendix A provides a position statement on progress against all HMIC recommendations. Those recommendations that have been implemented and are GREEN and which have previously been reported to Members of the Police Performance and Resource Management Sub Committee are not included.

**Contact:**

**Stuart Phoenix**

*Strategic Development - T: 020 7601 2213*

*E: [Stuart.Phoenix@cityoflondon.pnn.police.uk](mailto:Stuart.Phoenix@cityoflondon.pnn.police.uk)*

This page is intentionally left blank

## APPENDIX A - HMIC Report Recommendations

V.3 Position as at 08/09/2015

Traffic Light Colour	Definition
<b>GREEN</b>	The recommendation is implemented
<b>AMBER</b>	The recommendation is subject to ongoing work and monitoring
<b>RED</b>	The recommendation should have been implemented but has not been and is overdue
<b>WHITE</b>	The recommendation is dependent upon another organisation delivering a product.

### Joint Inspection of the Provision of Charging Decisions

A national report

Published May 2015, a joint inspection by HMIC and HMCPSI

Total of 8 actions, of which 5 are national and outside the remit of City of London Police.

3 actions relevant to the City of London Police, all of which have been completed.

Recommendation	Status	Due Date	Comment
1 CPS Area managers ensure all appropriate administrative staff are trained effectively to ensure CPS Direct records of charging decisions are uploaded correctly onto the CPS case management system	NA		This is action is for the CPS
2 The criminal justice business area committee of the National Police Chiefs' Council and the CPS revise the performance data used as part of the prosecution team performance management process to ensure they capture essential charging information	NA		This is action is for the CPS

**NOT PROTECTIVELY MARKED**

3	Police forces ensure that there are sufficient trained decision-makers available to ensure that timely high quality decisions are made in accordance with the Code for Crown Prosecutors and the Director's Guidance on Charging	<b>GREEN</b>		This subject is included in the Sergeants' Custody course. CID DS undertake this function
4	The College of Policing, in conjunction with the CPS, produces a set of national learning standards, for local delivery, which as a minimum includes: <ul style="list-style-type: none"> <li>• the operation of the Director's Guidance on Charging;</li> <li>• the Code for Crown Prosecutors; and</li> <li>• the content of Charging Reports and the National File Standard</li> </ul>	<b>NA</b>		This action is for the CPS and College of Policing
5	All police forces have effective processes for the supervision and management of pre-charge bail in accordance with Authorised Professional Practice	<b>GREEN</b>		Current practice in CoLP reflects APP
6	CPS Areas, in consultation with their aligned police forces, set out clearly the arrangements for the provision of early investigative advice	<b>NA</b>		This action is for the CPS
7	The criminal justice business area committee of the National Police Chiefs' Council and the CPS review the Director's Guidance on Charging to assess whether the range of offences the police can charge needs to be amended	<b>NA</b>		This action is for the CPS & NPCC
8	The rationale for police decisions to take no further action or proceed by way of an out of court disposal be recorded with the following information: <ul style="list-style-type: none"> <li>• the decision-maker's application of the full Code for Crown Prosecutors test; and</li> <li>• in relevant cases, consideration of the gravity matrix.</li> </ul> and, that wherever possible, that record is included on the MG3 form	<b>GREEN</b>		This is currently reflected on the MG3



## Joint Review of Disability Hate Crime Follow-up

A national report, published May 2015, a joint inspection by HMIC, HMCPSP and HMI Probation

Total of 7 actions, of which 6 are national and outside the remit of City of London Police.

1 action is relevant to the City of London Police, which is still in progress.

Recommendation		Status	Due Date	Comment
1	The police, CPS and probation trusts should adopt and publish a single, clear and uncomplicated definition of a disability hate crime that is communicated effectively to the public and staff	NA		This is action is for the Police, CPS and Probation Trusts at a national level
2	The police, CPS and probation trusts, when developing their strategic aims, should consider disability hate crime and the need for its reporting to be increased	NA		This is action is for the Police, CPS and Probation Trusts at a national level
3	The police, CPS and probation trusts should consider how their front-line staff participate in effective disability hate crime training to improve (as appropriate) investigative, prosecution and rehabilitation skills	NA		This is action is for the Police, CPS and Probation Trusts at a national level
4	It is in the interest of each police force to review the different methods by which information is received from the public to ensure that every opportunity is being taken to identify victims of disability hate crime	AMBER	Sep 2015	The Crime Directorate have commenced an initial assessment; work being rolled out includes awareness raising campaigns for the public and officers taking reports of crimes.
5	Regular checks should be put in place to ensure the accuracy of all CPS data relating to disability hate crime	NA		This is action is for CPS
6	Advocates should refer to section 146 of the Criminal Justice Act 2003 as part of the sentencing process (where appropriate) and the application/outcome should be recorded	NA		This is action is for CPS
7	Disability hate crime must have a higher priority within the work of probation trusts. They should put in place procedures to ensure that offender managers preparing pre-sentence reports have all necessary CPS case papers available to them and ensure that plans, where relevant, always contain (a) objectives to address victim safety/victim awareness and (b) manage the risk posed by the offender to the victim or other potential victims	NA		This is action is for Probation Service providers

## Stop and Search Powers 2

This was a national inspection  
The report was published March 2015.

Total of 11 actions, of which 8 are national and outside the remit of City of London Police.  
3 are actions relevant to the City of London Police  
2 have been completed, one remains in progress.

Recommendation		Status	Due Date	Comment
1	With immediate effect, while changes to the Authorised Professional Practice are being considered, the College of Policing should publish a working definition of what constitutes an effective and fair stop and search encounter.	NA	Immediate	This action is for the College of Policing
2	Chief constables should, with immediate effect, develop plans that set out how each force will complete the action required to make good progress in relation to the recommendations in HMIC's 2013 report, and publish these plans so that the public can easily see them on their websites. These plans should include the action forces are taking to comply fully with the Best Use of Stop and Search Scheme, initiated in April 2014 by the Home Secretary.	GREEN	Immediate	This was has been published on the City of London Police external website.
3	Within twelve months, chief constables and the College of Policing should agree and implement a set of minimum recording standards for the police use of the Road Traffic Act 1988 power to stop motor vehicles and the Police Reform Act 2002 powers to search for and seize alcohol and tobacco from young people for the purpose of assessing their effective and fair use.	WHITE	March 2016	This action is for the College of Policing and National Police Chiefs Council before CoLP can implement

**NOT PROTECTIVELY MARKED**

Recommendation		Status	Due Date	Comment
4	Within twelve months, the Home Office should establish a requirement for sufficient data to be recorded and published in the Annual Data Requirement to allow the public to assess how effective and fair the police are when they use these powers.	NA	March 2016	This action is for the Home Office
5	Within twelve months, the Home Office should incorporate the Road Traffic Act power to stop motor vehicles and the Police Reform Act Powers to search for and seize alcohol and tobacco into Code A, so that officers are provided guidance about how they should use these powers in the same way that Code A provides guidance about stop and search powers.	NA	March 2016	This action is for the Home Office
6	Within twelve months, the College of Policing should make sure that the relevant Authorised Professional Practice and the stop and search national training curriculum include instruction and guidance about how officers should use the Road Traffic Act 1988 power to stop motor vehicles and the Police Reform Act 2002 powers to search for and seize alcohol and tobacco from young people in a way that is effective and fair.	NA	March 2016	This action is for the College of Policing
7	Within three months, chief constables should require their officers to record all searches which involve the removal of more than an outer coat, jacket or gloves. This record must specify: the clothing that was removed; the age of the person searched; whether the removal of clothing revealed intimate parts of the person's body; the location of the search including whether or not it was conducted in public view; and the sex of the officers present.	GREEN	June 2015	The Standard Operating Procedure and forms have been amended to include this information.
8	Within twelve months, the Home Office should incorporate into Code A a requirement for the recording of all searches which involve the removal of more than an outer coat, jacket or gloves and a requirement for officers to seek the authority of a supervising officer before strip searching children.	WHITE	March 2016	This action is for the Home Office

**NOT PROTECTIVELY MARKED**

Recommendation		Status	Due Date	Comment
9	Within twelve months, the Home Office should work with forces to establish a requirement for sufficient data to be published in the Annual Data Requirement to allow the public to see whether or not the way that police conduct searches that involve the removal of more than an outer coat, jacket or gloves is lawful, necessary and appropriate.	<b>WHITE</b>	March 2016	This action is for the Home Office
10	Within three months, chief constables should put in place a process to report, at least once a year, the information they get from recording searches that involve the removal of more than an outer coat, jacket or gloves to their respective police and crime commissioners and to any community representatives who are engaged in the scrutiny of the use of stop and search powers to help them assess whether these searches are lawful, necessary and appropriate.	<b>RED</b>	June 2015	There remains a technical issue with searching and creating reports on BOBS system, which is unlikely to be rectified before the introduction of a new crime recording system. However, implementation of the mobile data solution should allow for this information to be extracted and reported.
11	Within twelve months, the College of Policing should make sure that the relevant Authorised Professional Practice and the stop and search national training curriculum include instruction and guidance about how to make sure that searches that involve the removal of more than an outer coat, jacket or gloves are conducted in a way that are lawful, necessary and appropriate.	<b>WHITE</b>	March 2016	This action is for the College of Policing to revise APP before CoLP can implement

## Welfare of Vulnerable People in Custody

A national report

The report was published March 2015

Total of 18 actions of which 11 are national and outside the remit of City of London Police.

7 are actions relevant to the City of London Police, of which 0 have been completed,

7 are still progress details below:

	Recommendation	Status	Due Date	Comment
1	A national group, with a set timeframe, chaired by the Home Office, should oversee implementation of these recommendations. One of the first tasks of this group should be to ensure implementation timescales are attached to these recommendations.	NA		This action is for the Home Office
2	<p>To improve transparency and public accountability... and to enable better management of custody practice, we recommend that police forces collect and publish data on police detention. The Home Office should work with forces to pilot a data collection series before including this as part of the mandatory Annual Data Return. As a minimum the data should include (collated by gender, race and ethnicity and age):</p> <ul style="list-style-type: none"> <li>• levels of stop and search, arrest and detention;</li> <li>• use of police custody as a place of safety under section 136 of the Mental Health Act 1983;</li> <li>• use of police custody as a place of safety under the Children Act 1989;</li> <li>• levels of strip-searching, use of force and other control measures (with information on the means used – see also recommendation 7);</li> <li>• numbers of children who are detained in police custody and for how long;</li> <li>• numbers of requests for children to be transferred to local authority accommodation under PACE; and</li> <li>• numbers of children actually transferred to local authority accommodation.</li> </ul>	GREEN	July 2015	The data required has been discussed at Custody User Group and will be produced by the Performance Analysis Manager within FIB and Custody Manager. The systems have been agreed and set up to extract the data and will be reported to the Police Performance and Resource Management Sub Committee.

**NOT PROTECTIVELY MARKED**

Recommendation		Status	Due Date	Comment
3	Regular reports on custody, including the data above, should be provided routinely by forces for consideration by the police and crime commissioner and be published on PCC's websites, to demonstrate to the public that the police are delivering services to communities on a fair and transparent basis	<b>GREEN</b>	July 2015	It has been agreed to supply this information to the Police Performance and Resource Management Sub Committee twice yearly.
4	<p>Relevant national policing leads building on recent work of the College of Policing on how demands on police forces are changing should take the lead in designing an audit process for use within each force, to quantify, with associated costs incurred:</p> <ul style="list-style-type: none"> <li>• time spent by officers in responding to, or managing incidents involving people in need of specialist mental health care, both inside and outside the custody suite. Where this occurs in custody, this should be quantified as the time the detainee remains in custody following a request by custody staff to specialist mental health services for assistance or transfer of the detainee to hospital; and</li> <li>• time spent safeguarding children in custody who have been referred to, but refused local authority accommodation.</li> </ul> <p>This information should be used to inform local Joint Strategic Needs Assessments, assess how far resources are allocated effectively to operational demand, and determine the potential benefits of a more integrated approach to delivery of the services, including joint commissioning of services.</p>	<b>NA</b>		This action is for national leads
5	The College of Policing should develop standards across the police service for the assessment of vulnerability in custody, as a basis for risk assessment, according to the vulnerability identified.	<b>NA</b>		This action is for the College of Policing
6	<p>The College of Policing should review its guidance to the police service on the use of force in relation to vulnerable people to reflect and align it with:</p> <ul style="list-style-type: none"> <li>• evidence across different sectors on best practice on the de-escalation of incidents;</li> <li>• the provisions of the Mental Capacity Act 2005, and related guidance, on the use of restraint for people who lack capacity to make decisions required in their own best interests; and</li> <li>• guidance across different sectors produced by the Independent Advisory Panel on Deaths in Custody on common principles for safer restraint.</li> </ul>	<b>NA</b>		This action is for the College of Policing

**NOT PROTECTIVELY MARKED**

Recommendation	Status	Due Date	Comment
<p>7 The police service, with the support and guidance of the College of Policing and the appropriate national policing leads, must establish a definition and a monitoring framework on the use of force by police officers and staff, linked to forces' risk registers. At a minimum this should ensure that:</p> <ul style="list-style-type: none"> <li>• more frontline officers and staff are trained in de-escalation skills;</li> <li>• there is a common understanding, informed by College of Policing Authorised Professional Practice on definitions of restraint and thresholds for the purposes of record-keeping;</li> <li>• the use of force in custody is recorded on CCTV and/or body worn cameras, and the recordings are monitored by senior managers, and made available to National Preventative Mechanism-visiting bodies as required; and</li> <li>• data collected on the use of force is monitored routinely, examined for trends, reported to police and crime commissioners and published on force websites to promote transparency and accountability to community groups and the wider population.</li> </ul>	<b>AMBER</b>	Dec 2015	<p>Personal safety training has been enhanced and is being delivered between July – December 2015.</p> <p>Discussions are taking place as to the frequency this information is reported to Police Committee</p>
<p>8 The College of Policing, in collaboration with relevant health and social care partners, should promote a joint, multi-agency approach to training for frontline staff, including those working in custody, on practical ways to support diversion from custody, vulnerability assessment and risk management. At a minimum, this should address:</p> <ul style="list-style-type: none"> <li>• a shared understanding of vulnerability, its identification and warning signs;</li> <li>• statutory roles and responsibilities, particularly as this is relevant to diversion from police custody;</li> <li>• the health and social care needs of vulnerable people in police detention, and associated requirements to be able to communicate well with them; and</li> <li>• proposals on the practicable implementation and governance of provision, oversight and evaluation of training at a local level.</li> </ul>	<b>NA</b>		<p>This action is for the College of Policing</p>

**NOT PROTECTIVELY MARKED**

Recommendation		Status	Due Date	Comment
9	<p>Police forces should establish a race equality governance framework linked to the force's risk register. This framework should include:</p> <ul style="list-style-type: none"> <li>• collection of core data sets by ethnicity as set out in recommendation 1;</li> <li>• development of a common understanding of the current situation through analysis of the data and engagement with Independent Advisory Groups and local communities;</li> <li>• plans to make improvements to practice where this is identified as being necessary; and</li> <li>• establishing appropriate leadership and governance structures to oversee and make sure the work is carried out.</li> </ul>	<b>AMBER</b>	Nov 2015	The data required by this recommendation is now being collated and will be reported to Committee and the IAG. The Equality and Inclusion sergeant will now work with UPD to ensure there is governance mechanism (possibly QoS Board) in place to act on analysis of the data ensure work is implemented.
10	<p>Police forces must comply with their duties to promote equality, as required in the Equality Act 2010, and:</p> <ul style="list-style-type: none"> <li>• recruit and promote people who have an interest in doing so;</li> <li>• monitor recruitment against the protected characteristics, seeking to have a workforce that reflects the communities in which the force operates; and</li> <li>• carry out and publish robust equality impact assessments across custody operations, which include an element of external challenge, and use these to develop improvement action plans and address any issues of discriminatory treatment.</li> </ul>	<b>GREEN</b>	July 2015	Recruitment related recommendation reflects existing practice. An existing has been reviewed and consultation with the IAG planned.
11	<p>Police forces should be included as members of all Health and Wellbeing Boards in England and equivalent local partnership boards in Wales. These local bodies should have a local focus on reducing unnecessary use of police custody through inter-agency needs assessment and service planning. This will be supported in practice by:</p> <ul style="list-style-type: none"> <li>• establishing a sub group focused on custody for each local body; and</li> <li>• clarifying accountabilities between these local oversight bodies and those with responsibility for commissioning services, both in the NHS and in local authorities.</li> </ul>	<b>GREEN</b>	July 2015	The Custody Inspector attends the Corporation's 'Healthy Behaviours' Board. They are also part of the Substance Misuse Partnership team, which together with G4S, Health Care Professionals and L&D which considers custody issues and clarifies roles and responsibilities in this area.



**NOT PROTECTIVELY MARKED**

Recommendation	Status	Due Date	Comment
12 The Home Office and the Department of Health should clarify the relationship between Health and Wellbeing Boards (and equivalent local partnership boards in Wales) and local commissioning bodies to ensure that police forces, local health and social care services are held to account for the provision of services to divert vulnerable adults away from custody and/or, as required in law, to vulnerable adults in custody.	<b>NA</b>		This action is for the Home Office
13 National work on mental health liaison and diversion and on street triage services should be used as the foundation for development of an evidence-based, integrated model of mental health crisis care, jointly commissioned and provided by the NHS, local authority social services, housing services and the police service. There should be an explicit duty between these agencies, in the interests of efficiency, to achieve collectively the aim of diverting people with mental health needs away from police custody and the criminal justice system. The model of care must include access to services for children in all cases.	<b>GREEN</b>	August 2015	2 specialist mental health care professionals are now working with the Force as part of the Liaison and Diversion scheme that was launched in August 2015.
14 Local Safeguarding Children’s Boards (LSCBs) should hold police forces and local authority children’s services to account for the provision of services to divert children away from custody and provide support as required in law to children in custody. Police forces urgently should work with local authorities and LSCBs to: <ul style="list-style-type: none"> <li>• develop joint strategies that equip frontline staff to manage the behaviour of children looked after by the local authority so that detention is a last resort;</li> <li>• ensure that no child who is looked after by the local authority is denied accommodation by them;</li> <li>• share data, as collected under recommendation 1, to inform local joint strategic needs assessments on safe accommodation requirements for children;</li> <li>• record and report to the LSCB the number of children held in custody (and their legal status), the efforts made to secure alternative accommodation and the reasons for failing to do so (with plans to address them); and</li> <li>• promote joint engagement with local Magistrates’ Associations to support a common, cross-agency understanding of relevant terminology, in particular the distinction between ‘safe’ and ‘secure’ accommodation.</li> </ul>	<b>NA</b>		This action is for the Local Safeguarding Children’s Boards

**NOT PROTECTIVELY MARKED**

Recommendation	Status	Due Date	Comment
<p>15 The College of Policing must work with the Association of Independent LSCB chairs to develop national guidance and protocols with the objective of reducing the criminalisation of children, particularly those looked after by local authority children’s social care services. At a minimum this should include:</p> <ul style="list-style-type: none"> <li>• guidance to police and local authorities on evidence-based preventive action;</li> <li>• guidance to police and local authorities on appropriate action in cases where children come to police attention;</li> <li>• guidance to chairs of local children’s safeguarding boards on good practice under section 38(6) PACE to promote consistency in holding the police service and local authorities to account; and</li> <li>• an expectation that police forces have a clear focus on children as a vulnerable group.</li> </ul>	<b>NA</b>		This action is for the College of Policing
<p>16 HMIC/HMIP should give consideration to including in the Expectations for Police Custody an expectation that no child is subjected to a strip-search unless the search is intelligence-led and authorised by an officer of inspector rank or above..</p>	<b>NA</b>		This action is for HMIC and HMIP
<p>17 The business of the National Preventive Mechanism Children and Young People’s Sub Group should include a focus on children in police custody, particularly on how effective local diversion arrangements and related public service safeguarding responsibilities are in respect of children.</p>	<b>NA</b>		This action is the National Preventative Mechanism Children and Young People Sub Group
<p>18 HMIC/HMIP must undertake a review of the methodology and expectations for inspections of police custody in the light of the findings of this thematic work. In particular we recommend that:</p> <ul style="list-style-type: none"> <li>• the Expectations for Police Custody are extended to include a view of custody from the first point of contact and other risks to the welfare of vulnerable detainees’ as identified in this inspection; and</li> <li>• the data collection undertaken in this inspection is developed to establish a ‘key statistics for police custody’ dataset, reflecting Equality Act 2010 protected characteristics, published at force level in inspection reports, and aggregated nationally for publication on HMIC’s website.</li> </ul>	<b>NA</b>		This action is for HMIC and HMIP

## Investigation and Prosecution of Fatal Traffic Incidents

A national report, published February 2015, a joint inspection by HMIC and HMCPsi

Total of 15 actions, of which 11 are national and outside the remit of City of London Police. 4 are actions relevant to the City of London Police, all of which have been completed.

Recommendation		Status	Due Date	Comment
1	Police disclosure officers must ensure that all disclosure schedules prepared include policy and strategy logs.	GREEN		This is current practice
2	Police forces should ensure that the most effective and appropriate resources are deployed to the scene of collisions which involve or may involve a fatality by arranging that: <ul style="list-style-type: none"> <li>officers dispatched to the scene have the necessary training and equipment to perform the role effectively; and</li> <li>specialist resources required are readily available to the senior investigating officers at the scene</li> </ul>	GREEN		There is 24/7 roads policing capability.
3	Police forces should ensure that police officers performing the role of family liaison officer have adequate time to perform their role effectively.	GREEN	July 2015	The SOP has been reviewed and managers reminded of obligations on FLOs prior to any abstraction being considered.
4	Police forces should ensure that family liaison officers involved in road death investigations have regular mandatory checks by occupational health departments.	GREEN		Annual mandatory checks are undertaken by Occupational Health
5	The College of Policing should include road death investigation within the Professionalising the Investigation Process (PIP) levels of investigation and make the training programme accessible and relevant to all road death investigators	NA		This action is for the College of Policing
6	The College of Policing should develop and promote: <ul style="list-style-type: none"> <li>an accreditation process for all road death investigators; and</li> <li>national training standards for all road death investigation personnel</li> </ul>	NA		This action is for the College of Policing

**NOT PROTECTIVELY MARKED**

Recommendation		Status	Due Date	Comment
7	CPS Headquarters should prescribe minimum standards and a common model organisational structure for handling fatal road traffic incident cases in every CPS Area, which should promote the role of specialist prosecutors by setting out eligibility criteria, accreditation and continuing professional development requirements.	NA		This action is for the CPS
8	CPS Headquarters should appoint a specialist fatal road traffic incident coordinator in each CPS Area including CPS Direct, and set clear expectations for the role and what it is expected to deliver.	NA		This action is for the CPS
9	CPS Headquarters should commission a skills audit and the development and delivery of a bespoke training programme to equip specialist fatal road traffic incident prosecutors, and those senior prosecutors designated to authorise key casework decisions, with the knowledge and skills they need to make appropriate decisions and communicate with bereaved families.	NA		This action is for the CPS
10	CPS Headquarters should issue guidance to prosecutors on the circumstances in which it is appropriate to charge assaults that arise from driving a motor vehicle.	NA		This action is for the CPS
11	CPS Headquarters should now review the requirement for approval of all decisions on charging to be made by Deputy Chief Crown Prosecutors or other senior lawyers and if it is to be retained, all senior prosecutors so designated must undertake the programme recommended at paragraph 4.16 of the report.	NA		This action is for the CPS
12	CPS Headquarters should add a reference to the Criminal Practice Direction on acceptance of pleas in its guidance on charging driving offences.	NA		This action is for the CPS
13	CPS Headquarters should facilitate the flagging of all fatal road traffic incident cases on the case management system (CMS) as a separate case category and mandate the collection of statistical and performance data at Area level, publishing this on a regular basis so that future training programmes can be informed by learning points derived from case reviews	NA		This action is for the CPS
14	CPS Headquarters should modify the Appeals and Review Unit's (ARU) practice of creating a separate case file on the case management system (CMS) where an appeal or Victims' Right to Review (VRR) referral has taken place as it unreasonably restricts access by the CPS Area staff to all records of review and other case material.	NA		This action is for the CPS

**NOT PROTECTIVELY MARKED**

Recommendation		Status	Due Date	Comment
15	CPS Headquarters should require all Areas to agree a standard protocol with minimum content with each police force in their region and meet regularly to review its effectiveness.	NA		This action is for the CPS

## Integrity Matters

A National report. Published January 2015 Total of 14 actions of which 5 are national and outside the remit of City of London Police. 9 were actions relevant to the City of London Police, all of which have been completed.

Recommendation		Status	Due Date	Comment
9	By 31 August 2015, all forces should ensure that their policies on the acceptance of gifts and hospitality comply with the national guidelines. By the same date, all officers and staff should be reminded of the policies.	GREEN	Aug 2015	Policy and SOP accord with national guidance, have been republished and staff required to read them using Triple A system.
12	By 31 August 2015, all forces should ensure they have the necessary capability and capacity to develop and assess corruption-related intelligence in accordance with the authorised professional practice.	GREEN	August 2015	The Force maintains an adequately resourced Counter Corruption Unit to discharge this function.
13	By 31 August 2015, all chief constables should satisfy themselves that they have processes in place to ensure that investigations into misconduct by officers and staff resulting in “no further action” are fair and free of any form of discrimination.	GREEN	August 2015	Peer reviews in place – conducted by HR
14	By 31 August 2015, all forces should ensure that there is sufficient analytical capability to analyse threats, risks, harms and trends in respect of misconduct, criminality and corruption in support of professional standards departments and anti-corruption units.	GREEN	August 2015	CoLP has analytical capability within PSD

## Police Integrity & Corruption

This was a City of London Police specific report  
Published November 2014

Total of 4 actions

Of these 0 are national and outside the remit of City of London Police.

4 were actions to the City of London Police, all of which have been completed

This action plan is now complete and will not be reported upon in future.

## Crime Inspection 2014

This was a City of London Police specific report  
Published November 2014

Total of 3 actions, all of which have been completed. Below is the final one that was previously outstanding.

Recommendation	Status	Due Date	Comment
3 Within 3 months, the City of London Police should develop and commence the implementation of a plan to improve the quality of victim services and contact beyond that already provided to victims supported by the vulnerable victim co-ordinator role within the public protection unit.	GREEN	February 2015	A Force victim charter setting out standards that victims can expect from the Force and which will improve victim services has been published and is being implemented. This is complemented by a funded post within ECD to cater specifically for the victims of fraud and a draft strategy aimed at improving the experience of victims of fraud nationally has been produced.

## Undercover Policing

A national report, published October 2014

Total of 49 actions, of these 32 are national and outside the remit of City of London Police.

15 were actions relevant to the City of London Police, of which 12 have been completed, 3 are still in progress.

Recommendation		Status	Due Date	Comment
17	Chief constables should establish and promulgate standard operating procedures to be adopted by all forces and other law enforcement agencies in accordance with the Authorised Professional Practice.	WHITE		Force SOP exists, however, APP not released so compliance with APP provisions cannot currently be assessed.
30	Chief constables and the heads of law enforcement agencies should enforce a consistent and fair reintegration strategy to enable undercover officers to return to other policing or agency duties.	WHITE	May 2016	A College of Policing working group has been set up to consider this nationally, any Force strategy will need to reflect the findings of the CoP. They have to report by March 2016, therefore the due date has been amended to 2 months following that date. Current Force practice is compliant with existing guidelines on re-integration.
49	Chief constables and the heads of law enforcement agencies should review their force or agency's approach to the use of undercover online policing and in every case ensure compliance with the Strategic Policing Requirement.	WHITE		This has been discussed with the College of Policing. APP covering undercover online activity is not available at this time. CoLP does not currently have an SOP for this area, however, practice complies with the provisions of the SPR. The Force will

**NOT PROTECTIVELY MARKED**

Recommendation	Status	Due Date	Comment
			revisit this area when APP is produced.



## Core Business, previously known as Making Best Use of Police Time

This was a national report, published September 2014.

Total of 40 actions, of which 3 are national and outside the remit of City of London Police.  
37 were actions relevant to the City of London Police of which 28 have been completed,  
9 are still in progress.

Page 133

Recommendation		Status	Due Date	Comment
2	Not later than 31 March 2015, all forces' planning documents should contain clear and specific provisions about the measures forces will take in relation to crime prevention, in accordance with the published national preventive policing strategy and framework and in discharge of chief constables' duties under section 8 of the Police Reform and Social Responsibility Act 2011 to have regard to the police and crime plans of their police and crime commissioners.	WHITE	March 2015	This is, in part, is dependent upon the publication of the National Preventative Policing Strategy and framework, which has still to be produced. However, the Policing Plan already contains specific provisions relating to prevention activities and there is a Force crime prevention strategy, therefore the Force has done everything it can at this stage to comply with this recommendation.
6	By 20 October 2014, the one force which has not already done so should adopt a sound force-level definition of a repeat victim of anti-social behaviour.	NA		This action does not relate to CoLP, which already uses a force-level definition of a repeat victim of ASB
15	Not later than 31 March 2015, all forces should establish and operate adequate processes for checking whether attendance data are accurate, including dip-sampling records.	RED	March 2015	The Force has processes in place to record attendance data. A process for confirming accuracy to include dip sampling remains in development. An update, including anticipated implementation will be reported to the Force Performance Management Group on 29 <sup>th</sup> Sep 2015.

**NOT PROTECTIVELY MARKED**

Recommendation		Status	Due Date	Comment
16	By 1 September 2015, all forces should work with the College of Policing to carry out research to understand the relationship between the proportion of crimes attended and the corresponding detection rates and levels of victim satisfaction.	WHITE	September 2015	College of Policing engagement with forces has not commenced.
26	All forces should work with the College of Policing to support its work to establish a full and sound understanding of the demand which the police service faces. Forces should understand what proportion of demand is generated internally and externally, and the amounts of time taken in the performance of different tasks. All forces should be in a position to respond to this work by 31 December 2015.	WHITE	December 2015	College of Policing engagement with forces has not commenced. However, CoLP has commenced its own programme of work around demand.
27	All forces should progress work to gain a better understanding of the demands they face locally, and be prepared to provide this to the College of Policing to establish good practice in this respect. All forces should inform HMIC of their progress on this matter through their annual force management statements.	AMBER	December 2015	Annual Force Management Statements (FMS) have not been released to forces at this time. Demand processes and data is currently being progressed in anticipation of the release of the FMS template.
29	All forces should work with the College of Policing to continue with its work to establish a full and sound understanding of the nature and extent of the workload and activities of the police service. All forces should be in a position to respond to this work by 31 December 2015.	WHITE	December 2015	College of Policing engagement with forces has not commenced.
32	All forces should work with the College of Policing to progress its work into how mental health cases and ambulance provision can be better managed. All forces should be in a position to respond to this work by 31 December 2015.	AMBER	December 2015	Contact made with College of Policing, internal work progressing. Demand information is currently being assessed.
33	All forces should work with the College of Policing to progress the work it has taken over from the Reducing Bureaucracy Programme Board to establish opportunities where savings can be made. All forces should be in a position to respond to this work by 31 December 2015.	WHITE	December 2015	College of Policing engagement with forces has not commenced.
36	By 1 September 2015, all forces should conduct a review into their use of video and telephone conferencing and ensure that it is being used wherever appropriate.	AMBER	September 2015	Work on this issue is being progressed as part of the Accommodation Programme and monitored through Force Change Board.

## Crime Data Integrity

This was a City of London Police specific report.

The report was published August 2014

Total of 10 actions, all of which have been completed.

Recommendation		Status	Due Date	Comment
3	The force should amend the procedure to transfer crimes to another force to include guidance on the transfer of evidential material.	GREEN	March 2015	The Force reviewed its procedures with other forces in relation to transfer of crimes. Guidance on the transfer of evidential material has been published.
4	The force should review the recording and quality assurance of the use of cannabis warnings to ensure they are only used in appropriate cases, are subject to effective supervisory oversight, and that the implications to the offender of accepting the warning are explained and recorded.	GREEN	Immediate	These requirements were incorporated into a revised Cannabis SOP, which has now been published.
10	The force should conduct a NCRS and HOCR training needs analysis. Immediately thereafter, it should introduce a tiered, co-ordinated training programme on NCRS and HOCR, prioritising personnel in roles which impact on quality, timeliness and victim focus. In particular, it should ensure the training is always made available to new personnel, including supervisors, during their induction to the control room.	GREEN	April 2015	The training needs analysis has been completed and training has started to be rolled out, which will continue into 2016.

Page 135

## Domestic Abuse

This was a national inspection with individual force recommendations. The report was published March 2014.

Total of 5 actions of which 4 have been completed, 1 is still in progress. Details below:

Recommendation		Status	Due Date	Comment
4	The force should make more effective use of body-worn cameras to capture early evidence of injuries and scene footage to strengthen the evidence base for prosecutions.	RED	June 2015	Deployment has been delayed due to technical and legal issues and will not now commence until Oct/Nov 2015

## Stop & Search

This was a primarily a national report, but specific force recommendations were made separately. The report was published July 2013.

This action plan incorporates new recommendations to comply with the principles of the Home Office “Best Use of Stop & Search” which the Force signed up to on the 26<sup>th</sup> August 2014.

### National Report

Total of 10 actions, of which 2 are national and outside the remit of City of London Police.

8 were actions relevant to the City of London Police, of which 6 have been completed, 2 are still in progress. Details below:

	Recommendation	Status	Due Date	Comment
1	Chief Constables and the College of Policing should establish in the stop and search Authorised Professional Practice document a clear specification of what constitutes the effective and fair exercise of stop and search powers, and guidance in that respect. This should be compliant with the code of practice.	WHITE		This action is for the College of Policing re Authorised Professional Practice. The Force will work with the CoP in whatever capacity it can to support delivery of this recommendation
4	The College of Policing should work with Chief Constables to design national training requirements to improve officers’: understanding of the legal basis for their use of stop and search powers; skills in establishing and recording the necessary reasonable grounds for suspicion; knowledge of how best to use the powers to prevent and detect crime; and understanding of the impact that stop and search encounters can have on community confidence and trust in the police. Specific training should also be tailored to the supervisors and leaders of those carrying out stops and searches.	WHITE		This action is for the College of Policing re Authorised Professional Practice. The Force will work with the CoP in whatever capacity it can to support delivery of this recommendation

**NOT PROTECTIVELY MARKED**

Recommendation		Status	Due Date	Comment
5	Chief Constables should ensure that officers and supervisors who need this training are required to complete it, and that their understanding of what they learn is tested.	AMBER	Will be determined following College of Policing rollout	The College of Policing are producing a training package, but this is not expected to be rolled out until January 2016
9	Chief Constables should introduce a nationally agreed form (paper or electronic) for the recording of stop and search encounters, in accordance with the code of practice.	AMBER	Will be determined following Chief Constables Council input	No national form exists. The Force awaits recommendations from the Chief Constables Council.

**City of London Police Recommendations**

**Total of 15 actions of which 10 have been completed, 5 are still in progress. Details below:**

Recommendation		Status	Due Date	Comment
2	Publish a force definition of an effective outcome from the use of stop and search powers.	WHITE	To be determined upon national guidance becoming available	The force awaits national guidance and discussion has been had with the Community Scrutiny Group
5	To analyse the effects of the use of stop and search powers on recorded and detected crime, including mapping of searches against crimes.	AMBER	October 2015	Rollout of the tablet devices in October 2015 will enable the mapping and analysis of Stop and Search
10	Ensure Officers respond to the new National Training Standard for Stop & Search.	WHITE	January 2016	The College of Policing is reviewing national training and is expected to rollout training in January 2016.

**NOT PROTECTIVELY MARKED**

Recommendation		Status	Due Date	Comment
11	Ensure Officers are fit to exert Stop and Search powers.	WHITE		The College of Policing will be introducing an assessment for officers. CoLP is awaiting its release.
15	Stop and search data added to force crime maps	AMBER	October 2015	Rollout of the tablet devices in October 2015 will enable the mapping and analysis of Stop and Search.

## An Unannounced Inspection Visit to Police Custody Suites

A joint inspection by HM inspectorate of Prisons and HM inspectorate of Constabulary  
This was a City of London Police inspection, the report was published November 2012

Total of 37 actions of which 34 have been completed,  
3 closed to be considered as part of any new Custody facility.

Recommendation		Status	Due Date	Comment
4	Arrangements in booking-in areas should allow for private communication between detainees and staff	CLOSED		Closed – to be considered as part of any new Custody facility
5	There should be designated adapted cells that have a lowered call bell.	CLOSED		Closed – to be considered as part of any new Custody facility
15	Suitable facilities should be provided for detainees to have exercise in the open air	CLOSED		Closed – to be considered as part of any new Custody facility
24	There should be a mental health liaison and/or diversion scheme to enable detainees with mental health problems to be identified and diverted in to appropriate mental health services as required.	GREEN	Mid April 2015	Liaison and Diversion arrangements commended on 17 <sup>th</sup> August 2015.

<b>Committee(s):</b>	<b>Date(s):</b>
Audit and Risk Management Committee	17 September 2015
<b>Subject:</b> Appointment of External Members	<b>Public</b>
<b>Report of:</b> The Town Clerk	<b>For Decision</b>
<b><u>Summary</u></b>	
<p>One of our 3 external Members, Hilary Daniels, has expressed a wish to serve the Committee again, when her current term expires in 2016. With over 20 year's extensive experience in working at Board level, in both Executive and Non-Executive roles, Hilary's contribution to the work of the Committee has been invaluable.</p> <p>Members are reminded that, at its meeting on 16<sup>th</sup> January 2014, the Court of Common Council agreed to vary the procedure to allow external members to be re-appointed for a further term, with 2 terms being the norm. In 2014, the Court agreed to allow the re-appointments of Kenneth Ludlam and Caroline Mawhood for 3 and 4 years respectively. Given that Hilary is prepared to serve another 3 year term, this has an additional benefit in that the terms of all 3 external members will expire at staggered intervals; i.e. 2017, 2018 and 2019.</p> <p><b>Recommendation, that:</b></p> <p>Members agree to re-appoint Hilary Daniels for a further term, expiring in March 2019.</p>	

## **Main Report**

### **Background**

At its meeting on 16th January 2014, the Court of Common Council agreed to vary the procedure to allow external members to be re-appointed for a further term. However, in the interests of maintaining a fresh perspective we recommended, and the Court subsequently agreed, that as the norm, a maximum of two terms be served. In 2014, the terms for Kenneth Ludlam and Caroline Mawhood were renewed for 3 and 4 years respectively.

### **Current position**

Hilary Daniels appointment is due to expire in 2016 and she has expressed a wish to continue serving for a further term, until 2019. This has an additional benefit in that the terms of all 3 external members will expire at staggered intervals; i.e. 2017, 2018 and 2019.

Hilary is a qualified accountant, with a particular interest in the regulation of the profession to ensure high technical and ethical standards in the public interest. With over 20 year's extensive experience in working at board level, in both Executive and Non-Executive roles, Hilary's contribution to the work of the Committee has been invaluable.

### **Conclusion**

Members are asked to note the content of the report and re-appoint Hilary Daniels for a 2<sup>nd</sup> term.

### **Background Papers**

Report to the Court of Common Council, 16 January 2014.

### **Contact:**

Julie Mayer  
[julie.mayer@cityoflondon.gov.uk](mailto:julie.mayer@cityoflondon.gov.uk)  
020 7 332 1410



<b>Committee(s):</b>	<b>Date(s):</b>
Audit and Risk Management	17 September 2015
<b>Subject:</b>	<b>Public</b>
Risk Management	
<b>Report of:</b>	<b>For Information</b>
The Chamberlain	

### Summary

This report seeks to give further assurance to Members in respect of the City of London Corporation's robust and effective risk management systems. Members of the Audit and Risk Management Committee (ARMC) have a key oversight role in ensuring that the Corporation's risk management framework and policies are firmly embedded and operating effectively and, recently, significant steps have been taken by both Officers and Members to strengthen this level of assurance.

In support of these actions, the Summit Group of Chief Officers have established a new Chief Officer Risk Management Group (CORMG), chaired by the Chamberlain, that is tasked with undertaking a robust and regular review of the Corporate Risk Register. This has already resulted in a more dynamic register, with more clearly specified mitigations, in support of management of the corporate risks. In the event of concerns being raised, CORMG will review the issue and report back to the next ARMC.

#### **Recommendations:**

Members of the Audit and Risk Management Committee are asked to:

1. Receive regular reports on the output of the work of the CORMG, to enable Members to consider their robustness of the review process. (In the event of concern(s) being raised, then CORMG will review the issue and report back to the next Committee.)
2. Review, at least annually, whether further steps should be taken to strengthen the robustness of the risk management framework.

### Main Report

#### **Background**

Members and officers of the Corporation are committed to ensuring that robust and effective risk management systems are in place. These systems should ensure that:

- There is clarity over the key strategic and departmental risks facing the Corporation.
- The ownership and responsibility for management of these risks is clearly identified.
- There are appropriate mitigations in place that will contain, and in most cases reduce, the risk threat over time.

- New potential/actual risks are identified at an early stage, as a result of an embedded 'risk' culture and appropriate escalation procedures.

## **Current position**

Members of the Audit and Risk Management Committee have a key oversight role in ensuring that the Corporation's risk management framework and policies are firmly embedded and operating effectively in a way that will achieve these goals. Significant steps have been taken by Members to strengthen the level of assurance by:

- Introducing Risk Challenge sessions with Chief Officers; in which Members invite Chief Officers to outline how they ensure risk is effectively managed within their departments.
- Re-introducing 'deep dives' on corporate risks to provide further assurance on the management of corporate and departmental risks.
- Ensuring all Grand Committees consider current 'red risks' at each meeting and review the departmental risk register, at least on a quarterly basis.

In support of these actions, the Summit Group of Chief Officers have established a new Chief Officer Risk Management Group (CORMG), chaired by the Chamberlain, that is tasked with undertaking a robust and regular review of the Corporate Risk Register and with making recommendations to Summit Group on the de-escalation of existing corporate risks and the timely escalation of new risks. This has already resulted in a more dynamic register, with more clearly specified mitigations in support of management of the corporate risks.

## **Conclusion**

The Summit Group of Chief Officers have established a new Chief Officer Risk Management Group (CORMG), chaired by the Chamberlain, which had resulted in a more dynamic register. In the event that concern(s) are raised, CORMG will review the issue(s) and report back to the next Audit and Risk Management Committee. The recommendations, as set out in this report, seek to clarify the position and give further assurance to Members.

**Dr. Peter Kane**  
**Chamberlain**

T: 020 7332 1300

E: [peter.kane@cityoflondon.gov.uk](mailto:peter.kane@cityoflondon.gov.uk)