Notice of Meeting

AUDIT AND STANDARDS COMMITTEE

Monday, 3 February 2020 - 7:00 pm
Council Chamber, Town Hall, Barking

Members: Cllr Princess Bright (Chair), Cllr Adegboyega Oluwole (Deputy Chair), Cllr Toni Bankole, Cllr Simon Bremner, Cllr Josie Channer, Cllr Rocky Gill, Cllr Mohammed Khan and Cllr Faraaz Shaukat

Independent Advisor: Stephen Warren

By Invitation: Cllr Dominic Twomey

Date of publication: 24 January 2020

Chris Naylor
Chief Executive

Contact Officer: Masuma Ahmed
Tel. 020 8227 2756
E-mail: masuma.ahmed@lbbd.gov.uk

Please note that this meeting will be webcast, which is a transmission of audio and video over the internet. Members of the public who attend the meeting and who do not wish to appear in the webcast will be able to sit in the public gallery on the second floor of the Town Hall, which is not in camera range.

To view webcast meetings, go to https://www.lbbd.gov.uk/council/councillors-and-committees/meetings-agendas-and-minutes/overview/ and select the meeting from the list.

AGENDA

1. **Apologies for Absence**

2. **Declarations of Interest**

3. **Minutes - To confirm as correct the minutes of the meetings held on 23 July 2019 (Pages 3 - 6)**

4. **Counter Fraud 2019-20, Q1 - Q3 and Counter Fraud Policies & Strategy Report (Pages 7 - 99)**

5. Internal Audit Report 2019/20 Q1 - Q3 (April to December 2019) (Pages 101 - 113)

6. Progress Update on External Audit of 2018-19 Accounts (Pages 115 - 117)

7. Corporate Risk Register Update (Pages 119 - 147)

8. Work Programme 2019/20 (Pages 149 - 156)

9. Any other public items which the Chair decides are urgent

10. To consider whether it would be appropriate to pass a resolution to exclude the public and press from the remainder of the meeting due to the nature of the business to be transacted

Private Business

The public and press have a legal right to attend Council meetings such as the Audit and Standards Committee, except where business is confidential or certain other sensitive information is to be discussed. The list below shows why items are in the private part of the agenda, with reference to the relevant legislation (the relevant paragraph of Part 1 of Schedule 12A of the Local Government Act 1972 as amended). ***There are no such items at the time of preparing this agenda.***

11. Any other confidential or exempt items which the Chair decides are urgent

Our Vision for Barking and Dagenham

ONE BOROUGH; ONE COMMUNITY; NO-ONE LEFT BEHIND

Our Priorities

A New Kind of Council

- Build a well-run organisation
- Ensure relentlessly reliable services
- Develop place-based partnerships

Empowering People

- Enable greater independence whilst protecting the most vulnerable
- Strengthen our services for all
- Intervene earlier

Inclusive Growth

- Develop our aspirational and affordable housing offer
- Shape great places and strong communities through regeneration
- Encourage enterprise and enable employment

Citizenship and Participation

- Harness culture and increase opportunity
- Encourage civic pride and social responsibility
- Strengthen partnerships, participation and a place-based approach

This page is intentionally left blank

MINUTES OF
AUDIT AND STANDARDS COMMITTEE

Tuesday, 23 July 2019
(7:32 - 8:58 pm)

Present: Cllr Princess Bright (Chair), Cllr Adegboyega Oluwole (Deputy Chair), Cllr Rocky Gill, Cllr Mohammed Khan and Cllr Faraaz Shaukat

Also Present: Stephen Warren

Apologies: Cllr Toni Bankole and Cllr Simon Bremner

1. Declarations of Interest

There were no declarations of interest.

2. Minutes (3 April 2019)

The minutes of the meeting held on 3 April 2019 were confirmed as correct.

3. Approval of the Statement of Accounts 2018/19

The Chief Operating Officer (COO) introduced a report on the Council's Statement of Accounts for 2018/19.

The draft accounts had been certified by the COO as presenting a true and fair view of the Council's financial position by the statutory deadline of 30 May 2019 and were now the subject of a detailed audit by the Council's new external auditors, BDO, who took up the role at the beginning of 2019.

Representatives of BDO were present and explained that there had been a number of challenges in conducting the audit which meant that the final accounts would not be able to be published by the 31 July deadline, although this would not have an impact on the timetable for the accounts being signed off of the individual Council-owned companies. The challenges included the production of an inaugural set of Group Accounts relating to the Council's subsidiary companies and discussions had taken place with Council officers regarding the work needed to be undertaken to the Group Accounts, as well as in several other areas, to enable the audit to be concluded. The COO added that although there was still much to be done, the audit was not expected to lead to the Council's final accounts being 'qualified' in any way.

During the discussions, Members raised a number of issues which included the cessation of Revenue Support Grant funding from 2021, the ongoing pressures on budgets and the consequential impact on the Council's reserves, the Council's borrowing arrangements and the 20% increase in complaints from the public during 2018/19 (which was referred to in the Annual Governance Statement). The BDO representative explained that the audit focussed on compliance with Council policies and accounting practice, value-for-money and 'reasonableness' considerations, the impact on the Council's medium-term financial strategy and the robustness of the arrangements, as opposed to the detail of individual decisions

taken by the Council.

With regard to the reserves and borrowing issues, the COO directed Members to the "Medium Term Financial Strategy and Reserves Policy 2019/20 to 2023/24" report to the Cabinet of 16 July 2019 and the "Treasury Management Annual Report 2018/19" to Assembly of 24 July 2019 for further information on those aspects. The COO was also pleased to confirm that the problems that had caused the 20% increase in complaints from the public during 2018/19, which primarily related to the domestic waste collection service, had been addressed and the number of complaints received had reduced significantly over the last few months.

In respect of the signing off of the final Statement of Accounts on the completion of BDO's audit, the Committee requested that the matter be brought back for its consideration rather than delegated to the COO and Chair, as had been proposed in the report. The Committee also asked that the final papers be circulated as far in advance as possible to allow Members and the Independent Advisor (Audit) (IAA) to fully consider the documentation. To that end, officers were asked to liaise with BDO regarding the expected audit completion date and, if appropriate, to arrange a special meeting of the Committee to consider the final Accounts prior to the next scheduled meeting on 28 October 2019.

The IAA acknowledged the particular challenges of this year that had led to the delays with the 2018/19 Statement of Accounts and proposed that progress / update reports on some of the documentation that made up the Statement of Accounts could be presented to the Committee during the course of the year, to enable Members to consider matters in more detail. One of those documents was the Annual Governance Statement and the IAA suggested that the document could benefit from being reviewed to make it more meaningful to a wider audience.

Having regard to the above, the Committee resolved to:

(i) Approve the draft Statement of Accounts for the year ended 31 March 2019 as appended to the report;

(ii) Agree that, on the conclusion of BDO's full audit, the final Statement of Accounts 2018/19 be presented to the Committee for formal approval prior to their publication.

4. External Audit 2018/19 Report

Following on from Minute 39 above, the Committee received a presentation from representatives of BDO, the Council's External Auditor, on the draft audit completion report in respect of the Council Pension Fund Accounts for 2018/19, which had been circulated to members and published to the Council's website on the day of the meeting.

Mr Indika of BDO referred to the approach taken to the audit and clarified matters in respect of 'materiality' and the risk assessment strategy underpinning the audit. It was noted that BDO anticipated issuing an unmodified opinion on the completion of the audit although there were some key matters that remained outstanding in respect of (i) the accounting treatment of £20m pre-paid contributions by the Council; and (ii) Pension Liability Valuation issues stemming from two recent Court

judgements, alongside a number of other 'non-material' outstanding matters as listed in the report. In response to Members' questions, the BDO representatives provided further information on the two key outstanding matters as well as the unadjusted audit differences amounting to £96,000, protection against Pension Fund fraud and the audit testing of employee contributions which had identified four cases of contributions being incorrectly calculated.

The Committee thanked BDO for the report and presentation.

5. Internal Audit Annual Report and Annual Governance Statement 2018/19

The Head of Assurance presented the Internal Audit Annual Report for 2018/19, alongside the draft Annual Governance Statement for 2018/19.

The Head of Assurance referred to the key elements of internal audit work undertaken during the year and his overall opinion for the year, which was that the Council's arrangements were ""generally satisfactory with some improvements required". In respect of those areas where improvements were required, there was one classification of 'no assurance' in relation to controls and processes within the Adoptions service, although it was noted that a follow-up audit had provided greater assurance. There were also a number of 'limited assurance' findings and the Committee noted that a common theme amongst them were outdated guidance and documentation. One example was in the area of recruitment and the Head of Assurance outlined some of the steps that had been taken to address the concerns, which included mandatory training for all recruiting managers, the updating of guidance manuals and the creation of the Workforce Board, chaired by the Chief Executive, which considered all recruitment and restructure proposals.

In response to Members' questions, the Head of Assurance explained that a risk-based approach was used to determine the areas to be audited in any one year and that the timetable for implementing improvements highlighted by an audit would vary depending on the scale and nature of the improvements required. With regard to the 'limited assurance' findings from five audits carried out during the year, the Head of Assurance agreed to provide further details to the next meeting of the Committee.

In respect of the draft Annual Governance Statement for 2018/19, it was noted that the document would be considered as part of the final Statement of Accounts report at the Committee's next meeting.

The Committee noted the Internal Audit Annual Report for 2018/19, as set out at Appendix 1 to the report.

6. Counter Fraud Annual Report 2018/19

The Head of Assurance introduced the Counter Fraud Annual Report for 2018/19, which set out details of the counter fraud work undertaken by the Internal Audit team during 2018/19 in relation to housing investigations and corporate fraud matters.

The team had received 246 referrals during the year in relation to corporate fraud activity, 43 of which were progressed to the investigation stage. With regard to

housing investigations, 166 new cases were received and all but 12 had been resolved by the year end. Of the 154 cases that were resolved, 14 Council properties were recovered for re-letting via the Council's housing waiting list and over £1m was saved.

In response to a question regarding a spate of cyber-attacks that had targeted the Council and schools in January 2019, the Head of Assurance explained the methods used by perpetrators and the additional resilience measures put in place by the Council, which included the blocking of the originating ISP addresses and reminders sent to all staff advising what to look out for and where to report any concerns.

The Committee noted the Counter Fraud Annual Report 2018/19.

7. Complaints against Members Update

The Committee received and noted the six-monthly update report regarding complaints against Members of the Council, which showed that the Monitoring Officer was currently progressing one complaint that had been received alleging a possible breach of the Councillors' Code of Conduct.

8. Audit and Standards Committee Work Programme 2019/20

The Committee noted the work programme for the remainder of the 2019/20 municipal year and officers confirmed that the additional reports that had been requested during the meeting would be built into the programme.

It was also suggested that the report to the next meeting include a table showing how the Committee would fulfil its terms of reference against the annual work programme.

AUDIT & STANDARDS COMMITTEE

3 February 2020

Title: Counter Fraud 2019/20 Q1 - Q3 (April to December 2019) and Counter Fraud Policies & Strategy Report	
Open Report	**For Decision**
Wards Affected: None	**Key Decision:** No
Report Author: Kevin Key, Counter Fraud Manager	**Contact Details:** Tel: 020 8227 2850 E-mail: Kevin.Key@lbbd.gov.uk
Accountable Director: Claire Symonds, Chief Operating Officer	

Summary:

This report brings together all aspects of counter fraud work undertaken to the end of Q3 of 2019/20. The report details progress and results to 31 December 2019.
To ensure proper arrangements to administer the Council's financial affairs, the Council has adopted key policies and a strategy to combat fraud and irregularity. These polices were approved by Cabinet and to further strengthen their importance, as part of robust governance, recommended for review annually.

Recommendation:

Members are asked to:

(i) Note the contents of the report and the Council's updated Counter Fraud Policies and Strategy; and

(ii) Commend its principles to school governing bodies, and where appropriate to other stakeholders, including partnerships, arm-length organisations, and to contractors.

1. Summary of counter fraud work undertaken to Quarter 3 2019/20

1.1 The tables below indicate the level of work completed in the two separate areas for which the team are responsible; Housing and Corporate Fraud.

2. Corporate Fraud Activity including Whistleblowing

2.1 The update on corporate fraud activity for Quarter 3, along with the yearly totals, is set out below. The team receives many referrals throughout each quarter and log and assess each case independently. A decision is then made as to what the best course of action is to deal with the referral. This means either the team will open an investigation, refer to another service block of the council or arrange for the matter to be referred to a specific manager for action.

2.2 Fraud referrals to date incl. whistleblowing:

	18/19 Total	Q1	Q2	Q3	19/20 Total
Cases Outstanding from last quarter		8	8	4	
Referrals received in Period	246	46	50	52	148
Cases accepted for investigation	43	15	11	8*	34
No further Action after initial review/already known	28	14	5	4	23
Referred to other service block within LBBD	165	17	34	40	91
DPA, FOI, and other information provided	76	11	14	12	37
Cases closed following investigation	38	15	15	7	37
Ongoing Corporate Fraud Investigations:		8	4	5	

***includes 2 referrals to Action Fraud*

2.3 The data demonstrates what action is being taken on every referral received. We have also added to the outcomes section referrals made directly to the Police/Action Fraud.

2.4 The referrals received relate to the number of cases that are sent through to the Fraud email inbox or where contact is made directly with members of the team. All contact is logged and assessed accordingly. Many referrals are sent through in the belief that fraud has been committed, but following assessment found to be better dealt with elsewhere.

2.5 We receive requests that relate specifically to CCTV, Subject Access, Freedom of Information and Data Protection as well as referrals relating to Housing Benefits, Council Tax, Department for Work & Pensions, Complaints, Parking Enforcement, Housing services, noise nuisance, Housing Association properties, Planning, Private Sector Licencing, Police matters and Trading Standards. In short, if there is a possible consideration of fraud we are likely to have received a referral either via email or phone.

2.6 Outcomes to date and yearly total 2019/20

	18/19 Total	Q1	Q2	Q3	19/20 Total
Recommended for disciplinary process/New cases as a result	3	1	1	0	2
Referred for Management action	10	6	3	3	12
No fraud/No further action	10	5	7*	2	14*
Referred to Police/Action Fraud		3	4	2	9

*includes 2 cases where no fraud identified but serious concerns raised with procurement process – Internal Audit to review.

3. Current / future key issues– Corporate

3.1 In relation to the remaining staff member, formally employed by Be First, final checks are being completed to establish whether there is enough evidence and justification to proceed with a criminal prosecution.

3.2 There have been further attempted cyber scams reported to the team. Staff appear to be referring the matter to the team which would suggest the publicity and work undertaken in Quarters 1 & 2 has worked in raising the profile of this issue.

3.3 The National Fraud Initiative results have recently been updated; a detailed breakdown of the results will be provided in a later report, however there has not been any substantial fraud identified yet.

4. Regulation of Investigatory Powers Act

4.1 The Regulation of Investigatory Powers Act regulates surveillance powers, thus ensuring robust and transparent frameworks are in place to ensure its use only in justified circumstances. It is cited as best practice that Senior Officers and Members maintain an oversight of RIPA usage.

4.2 The last inspection of RIPA was undertaken by the Office of Surveillance Commissioners in December 2016. The report was favourable, and all recommendations subsequently implemented. In September 2017 The Investigatory Powers Commissioner's Office took over responsibility for oversight of investigatory powers from the Interception of Communications Commissioner's Office (IOCCO), the Office of Surveillance Commissioners (OSC) and the Intelligence Services Commissioner (ISComm).

4.3 The current statistics are set out below following review of the central register, held by the Counter Fraud Manager. As per previous guidelines, RIPA authority is restricted only to cases of suspected serious crime and requires approval by a Magistrate.

(a) <u>Directed Surveillance</u>
The number of directed surveillance authorisations granted during Quarter 3 October 2019 – December 2019 and the number in force at 31 December 2019

Nil granted. Nil in Force.

(b) <u>Communications Information Requests</u>
The number of authorisations for conduct to acquire communications data (e.g. mobile phone data) during Quarter 3 October – December 2019

Nil granted. Nil in force.

4.4 LBBD have been scheduled to have a RIPA inspection on 23 July 2020. The Inspector has requested to meet with the SRO and at least one Authorising Officer. Arrangements have been made and officers requested to be available on this date.

4.5 Training will be undertaken for RIPA throughout January, February and March and once completed will form an update to the RIPA Policy scheduled for June 2020.

4.6 Following the training, arrangements will be made to publicise to all staff (through the staff briefing, managers' briefing and screen background) the appropriate use of any surveillance being undertaken and the process to be followed. This should ensure LBBD are in the best position for when the RIPA inspection is undertaken.

5. Housing Investigations

5.1 Members are provided specific details on the outcomes from the work on Housing Investigations. For 2019/20, outcomes are set out below.

5.2 2019/20 Housing Investigations to date:

Caseload	18/19 Total	Q1	Q2	Q3	19/20 Total
Open Cases brought forward		22	29	26	
New Cases Added	166	39	36	29	104
Cases Completed	154	32	39	34	105
Open Cases		29	26	21	

On Going Cases - Legal Action	Q1	Q2	Q3
Notices Seeking Possession served	1	0	0
No of Cases - Recovery of property	4	4	4

Outcomes - Closed Cases	18/19 Total	Q1	Q2	Q3	19/20 Total
Convictions	0	0	0	0	0
Properties Recovered	14	0	3	1	4
Successions Prevented & RTB stopped/agreed	15	7	12	13	32
Savings (FTA, Single Person CTax, RTB, Decant)	£1,075,995	£208,000	£310,826	£556,200	£1,075,026
Other Potential Fraud prevented/passed to appropriate service block incl Apps cancelled	58	8	12	8	28
Referral to others outside of LBBD	1	0	0	0	0
No further action required/insufficient evidence	66	17	12	12	41

5.3 In addition to the above other checks are routinely carried out and information provided to others. Below is an indication of the level of work undertaken:

	Q1	Q2	Q3	19/20 Total
Data Protection Requests	8	10	6	24
Education Checks	84	143	108	335

(n.b. education checks relate to assisting admissions in locating children or families to free up school places or confirm occupancy. Data Protection Requests are received from other local authorities, the police, and outside agencies and responses provided in accordance with GDPR).

6. Current / future key issues to be considered – Housing

6.1 Right to Buy money laundering checks have increased and are undertaken to ensure the source of any cash purchase element of a Right to Buy is from a reputable source. The team have also begun allowing the RTB team to shadow them on visits to show the officers the type of issues that come up and how they can be resolved.

6.2 Work is ongoing to complete a full data match for housing stock through CallCredit. The Housing Investigation Team will lead on the work once the matches are returned to us and work closely with colleagues in My Place to deal with any tenancy issues highlighted.

7. Policies

7.1 The Assurance & Counter Fraud Group maintains a suite of counter fraud policies and a strategy to support the Council's strong stance against fraud, thus maintaining proper arrangements for the Council's finances and assets.

7.2. The policies were approved by Cabinet in January 2012 in line with the Council's robust stance on governance and are to be reviewed annually by the Audit and Standards Committee. This report sets out the latest versions and a summary of their purpose. Following review, there have been changes made to the policies to reflect the evolving nature of the Council as well as reference made in the Whistleblowing Policy to the Modern Slavery Act 2015. Changes to the Regulation of Investigatory Powers Policy will also need to be made following officer training during 2019/20.

7.3. These policies apply to all officers of the Council. In the spirit of raising fraud awareness they will also be promoted to and where applicable applied by the Council's partners such as Elevate, the wholly/partially owned firms, contractors and schools.

7.4 A brief description of the purpose of each policies/strategy is set out in the table below. The latest version is set out in the Appendices to this report.

Appendix	Document	Brief Description
A	Counter Fraud Strategy	Sets out the Council's commitment to reducing opportunities for fraud and corruption across all council services and taking the strongest possible action against those who seek to defraud the Council.
B	Counter Fraud Policy including Fraud Response Plan	Sets out how the Council responds to fraud and the changing risk profile of fraud and Includes guidance on what to do if an employee suspects fraud.
C	Prosecution Policy	Sets out the Council's approach to seeking redress/sanction against those who seek to defraud the Council, linking to the Disciplinary rules where the perpetrator is a member of staff
D	Money Laundering Policy	Sets out the Council's commitment to ensuring compliance with the requirements of the Proceeds of Crime Act 2002, the Money Laundering Regulations 2007 & 2012 and Chartered Institute of Public Finance and Accountancy (CIPFA) guidance for Local Authorities on Money Laundering.
E	Whistleblowing Policy	In accordance with the Public Disclosure Act 1998 (as amended by the Enterprise and Regulatory Reform Act 2013), sets out how workers can raise serious or sensitive concerns about other members of staff, suppliers, or people who provide services with protection from harassment, victimisation or bullying as a result of them raising concerns.
F	Regulation of Investigatory Powers Policy	Sets out rules and procedures for undertaking and gaining authorisation for covert surveillance in accordance with the RIPA Act 2000 (as amended by the Protection of Freedoms Act 2012) and compliant with Human Rights & Data Protection Legislation
G	Bribery Act Policy	Sets out the Council's commitment to the prevention, deterrence and detection of bribery and to raise awareness with relevant officers linking with the already in place Employee Code of Conduct and rules on accepting gifts and hospitality

7.5 Counter Fraud Policies and the Strategy will be made available on the Council website and staff intranet. Awareness raising, training and briefings will also be targeted at specific groups of staff - identified from an ongoing project to refresh of the Council's fraud risk assessment - through channels such as face to face, e-bulletins/e-learning and posters on staff notice boards and computer screens.

8. Financial Implications

Implications completed by: Thomas Mulloy, Chief Accountant

8.1 The Corporate Counter Fraud team is fully funded for 2019/20.

9. Legal Implications

Implications completed by: Dr Paul Feild, Senior Governance Solicitor

9.1 The Accounts and Audit (England) Regulations 2015 section require that: a relevant authority must ensure that it has a sound system of internal control which—facilitates the effective exercise of its functions and the achievement of its aims and objectives; ensures that the financial and operational management of the authority is effective; and includes effective arrangements for the management of risk.

9.2 Furthermore the Director of Finance has a statutory duty, under Section 151 of the Local Government Act 1972 and Section 73 of the Local Government Act 1985, to ensure that there are proper arrangements in place to administer the Council's financial affairs.

9.3 Counter Fraud practices set out in this report address the need to counter fraud, money laundering, bribery and the proceeds of crime. The Councils policies guide on the investigatory and prosecution process. In formulating the policies, it addresses the issue of corruption and bribery. Corruption is the abuse of entrusted power for private gain. The Bribery Act 2010 defines bribery as "the inducement for an action which is illegal, unethical or a breach of trust. Inducements can take the form of gifts, loans, fees, rewards or other advantages whether monetary or otherwise".

9.4 The Local Government Act 1972 provides the Council with the ability to investigate and prosecute offences committed against it. We will enhance our provision further by making best use of existing legislation, for example the Proceeds of Crime Act 2002, to ensure that funds are recovered, where possible by the Council.

Public Background Papers used in the Preparation of the Report: None.

List of Appendices

A	Counter Fraud Strategy
B	Counter Fraud Policy including Fraud Response Plan
C	Prosecution Policy
D	Money Laundering Policy
E	Whistleblowing Policy
F	Regulation of Investigatory Powers Policy
G	Bribery Act Policy

This page is intentionally left blank

Counter Fraud Strategy

June 2019

Date Last Reviewed:	May 2019
Approved by:	Audit & Standards Committee
Date Approved:	TO BE ADDED
Review Date:	June 2020
Document Owner:	Finance Director

Counter Fraud Objective

To create a culture and organisational framework, through a series of comprehensive and inter-related procedures and controls, which maximises the deterrence of fraud, minimises the incidence & impact of fraud against the Council, and ensures, through professional investigation, effective outcomes including sanctions and redress against those who defraud the Council. The Strategy is based on the following principles:

Acknowledge responsibility The Council has ensured that fraud risks are managed effectively across the whole organisation.
Identify risks We use fraud risk to understand specific exposures, changing patterns in fraud and corruption threats and the potential consequences to the Council and its service users.
Develop a strategy We have set out the Council approach to managing fraud risks and defining responsibilities for action.
Provide resources We have appropriate resources to support the counter fraud strategy.
Take action We have a suite of policies to support the counter fraud strategy and act to deter, prevent, detect and investigate fraud.

Links to Corporate Objectives

The vision for the Borough is **One borough; one community; London's growth opportunity.** To achieve the Vision, the Council's priorities are:

- Encouraging civic pride
- Enabling social responsibility
- Growing the borough

This Strategy ensures resources are correctly applied in the provision of high quality services and initiatives that deliver these Corporate priorities.

Resources & Skills

The Assurance Group will investigate all issues of suspected fraud and irregularity and promote the counter fraud agenda through proactive and preventative activities. All investigators are professionally accredited and undertake appropriate continuous professional development. The authority for the Assurance Group to investigate is

enshrined in the Council's Constitution and Financial Rules and provide authority to have access to all records, and to all council premises.

Investigations into allegations of housing fraud allow staff to utilise powers under Section 4 of the Prevention of Social Housing Fraud (Power to Require Information) (England) Regulations 2014 as appointed Authorised Officers.

The Assurance Group has access to an Accredited Financial Investigator to enable redress under the Proceeds of Crime Act (POCA). Any monies recovered will be used to further promote counter fraud across the council.

Responsibility

The Assurance Group will champion the tough stance against fraud and promote counter fraud across the council, its Members, staff, contractors, partner agencies and service users. Professional investigators will work in accordance with relevant codes of practice and Council policies, while always maintaining confidentiality, complicity with the employee code of conduct and guidelines of relevant legislation.

Liaison

The Assurance Group will utilise all methods available to detect fraud. Arrangements are in place to actively participate in the National Fraud Initiative (NFI) as well as continuing to develop and support initiatives that involve the exchange of information and data matching between the Council and other agencies.

In addition, we will work with colleagues in other Local Authorities and utilise counter fraud networks such as LBFIG, LAG and CIPFA Counter Fraud Centre.

Taking Action and Supporting Polices

Deterrence

We will publicise our counter fraud measures to promote the deterrent message, including the effectiveness of controls including the governance framework, arrangements that are in place to detect fraud, the professionalism of those who investigate fraud, the Council's success in applying proportionate sanctions and the prompt, effective recovery of losses.

Prevention

The Assurance Group works to support management in assessing compliance with the Council's policies and ensuring that adequate levels of internal control are included in operational procedures. The Assurance Group will advise and promote awareness on the importance of considering fraud risks as part of good governance arrangements as well as managing the changing risk profile of fraud in order to tackle new areas.

Detection

In addition to maintaining channels for the report of fraud, the Assurance Group will proactively use all legal and cost-effective means to detect fraud, including working with other organisations and participating in national data matching schemes.

Investigation

We will investigate all allegations of fraud in line with our polices and adhering to relevant legislation. Outcomes from investigations will include recommendations as well as necessary changes to systems and procedures to ensure that similar frauds will not recur.

Recovery and Sanctions

Where fraud is identified we will seek to recover losses and prosecute or apply other sanctions to perpetrators. Where fraud by employees is indicated, then action will be taken in accordance with the Council's disciplinary procedures. This may be in addition to any civil recovery action or sanctions.

Redress

Compensation, or confiscation, under proceeds of crime legislation will be sought wherever appropriate in accordance with the Prosecution Policy. Our aim is to ensure that those who seek to defraud the Council do not profit from their criminal activity.

Policies

All Counter Fraud work will be undertaken in accordance with relevant policies as follows:

Counter Fraud Policy including Fraud Response Plan	Our commitment to reducing opportunities for fraud and corruption across our services and taking the strongest possible action against those who seek to defraud us.
Prosecution Policy	Our approach to seeking redress/sanction against those who seek to defraud the Council.
Money Laundering Policy	Our commitment to complying with the requirements of the Proceeds of Crime Act 2002, Money Laundering Regulations 2007 & 2012 and CIPFA guidance.
Whistleblowing Policy	Our commitment to the Public Disclosure Act 1998 and supporting staff who raise concerns about various serious issues.
Regulation of Investigatory Powers Policy	Our commitment to adhering to RIPA 2000 in relation to covert surveillance.
Bribery Act Policy	Our commitment to the Bribery Act 2010
Proceeds of Crime Act 2002 Policy	This Policy has moved to Regulatory Services under the financial Investigation Manager. The Policy sets out our approach to applying procedures under POCA.

Review & Assessment/Quality Assurance

The strategy and associated polices will be reviewed annually and assessed against best practice across local authorities. The outcomes from counter fraud work will be periodically reported to Members of the Audit & Select Committee and outcomes assessed to evaluate success.

Counter Fraud Policy

June 2019

Date Last Reviewed:	May 2019
Approved by:	Audit & Standards Committee
Date Approved:	TO BE ADDED
Review Date:	June 2020
Document Owner:	Finance Director

The Council's commitment to the Counter Fraud Policy

The London Borough of Barking & Dagenham, "the Council", carries out its responsibilities and delivers high quality services to the local community. The immense variety of service provision places the Council at risk of loss from fraud perpetrated both internally and externally. The Council takes a tough stance against Fraud and considers this Policy, and associated strategy, to be an integral part of our approach.

What are the aims and requirements of the Policy?

Where Fraud is found to occur, in any form, it will be dealt with rigorously in a controlled manner in accordance with the principles in the Counter Fraud Policy. It will be investigated fully, and the Council will prosecute all offenders, where appropriate, including Members, employees, contractors, agency staff, consultants, suppliers and partners.

Who is governed by this Policy?

The Counter Fraud Policy applies to all staff including, and not limited to, temporary staff, sessional staff, consultants and contractors. It also covers suppliers and those providing services under a contract with the Council in their own premises, for example, care homes and sheltered accommodation as well as anyone who seeks to commit fraud against the Council.

Executive Summary

The Counter Fraud Policy makes clear the Council's commitment to reducing opportunities for fraud and taking the strongest possible action against those who seek to defraud the Council.

Contents

Counter Fraud Policy

Counter Fraud Policy

The council is responsible for the proper administration of its finances. This not only includes direct income and expenditure but also monies administered on behalf of the Government, our clients and for which the Council is the responsible accountable body. Anyone can potentially commit fraud, both inside and outside the organisation, and this can be targeted on all sources of income and expenditure and our valuable assets.

The Council aims to set high standards of service provision and is committed to upholding the reputation of the Authority and maintaining public confidence in its integrity. The expectation is that Members (Elected Councillors) and staff, at all levels, will adopt the highest standards of propriety and accountability and will lead by example. That same expectation is extended to individuals and organisations that encounter the Authority insofar they will act with integrity and without intent, or actions, involving fraud.

To achieve its aims and objectives the Council will therefore take a firm stance against any individual, group or organisation committing acts constituting theft, fraud, corruption, financial irregularity or malpractice (or other form of wrongdoing), whether it is attempted against, from or within the Council. In fulfilling our responsibilities to protect the public funds we administer; the Authority recognises the responsibilities placed upon it by statute and will actively promote this Policy which is designed to:

- Promote standards of honest and fair conduct
- Encourage prevention of fraud
- Maintain strong systems of internal control
- Promote detection
- Take a tough stance against fraud and bring to justice all persons who commit acts of fraud against the Council
- Recover any losses incurred by the Council

The Counter Fraud Culture and Deterrence

The culture of the organisation is one of honesty, openness and opposition to fraud. Members play a key role in maintaining and promoting this culture. Specifically, the Audit & Standards Committee is responsible for promoting high standards of conduct by Members, employees, its contractors and partners.

Members have a duty to ensure that Council assets are adequately safeguarded from fraud and abuse and to ensure that the Council's powers, duties and responsibilities are exercised in an open fair and proper manner to the highest standards of probity.

The Members and employees are an important element in the Council's stance on fraud and corruption and they are positively encouraged to raise any concerns that they may have on these issues where they are associated with a Council activity.

Members of the public are also able to report concerns to appropriate Council officers or relevant external agencies such as the Police, External Audit, and the Local Government Ombudsman.

The Public Interest Disclosure Act 1998 provides protection for those who voice genuine and legitimate concerns through the proper channels. The Council has adopted a Whistleblowing Policy to ensure a defined route to bring alleged instances of fraudulent, unlawful or otherwise improper conduct to the Council's attention. As well as the Whistleblowing Officer, this can involve Fraud Team, or the employee's line manager or Divisional Director or, if more appropriate, an officer external to the individual's department.

An ongoing proactive programme of work, including counter fraud awareness training and support, will be undertaken each year, using a risk-based approach to prioritise areas inherently at risk from fraud, outcomes from which will be publicised as appropriate. A pound lost through fraud is a pound that is stolen from Barking and Dagenham residents and reduces the amount available to spend on delivering services to residents.

The underlying message is that this Council will not tolerate fraudulent activity.

Prevention – Managing the Risk of Fraud

Fraud is costly in terms of financial loss and reputational risk. The risk of loss can be reduced through robust preventive measures and procedures such as: Internal Control systems, Standing Orders & Financial Regulations, Employee Code of Conduct, Disciplinary Rules and a Members Code of Conduct

The Chief Operating Officer has been delegated powers to control and regulate the Council's finances. These include the promotion of systems and practices to minimise the risk of fraud. An important part of the control framework is the maintenance of an effective internal and external audit of the Council's finances that operate to the best practice standards at any given time.

Managers, Contractors, Employees & Members

The effective eradication of fraud starts with managers. It is the responsibility of all Council managers to ensure that they manage the risk of fraud within their respective work areas. Managers are expected to be fully conversant with fraud risks (internal and external) and maintain robust controls within their service areas to mitigate these, and when considering the risk of fraud, should take the following steps:

Identify the risk areas

Managers must establish which parts of the service are most vulnerable to fraud e.g. letting or managing contracts, handling cash, allocating or distributing grants, ordering equipment, paying invoices, validating documentary evidence in support of claims for benefits etc. Other risks include assessing declared staff interests and considering whether such interests conflict with the Council's interests or would undermine public confidence in the Council.

Allocate responsibility for the risk
Managers must identify who has responsibility for managing each risk and ensure that the officer concerned has adequate training, support and expertise to manage the risk effectively.

Identify the need for controls
Managers must evaluate the adequacy of existing controls and establish what further controls or changes are required to reduce or eliminate the risk of fraud. In addition, managers should utilise internal audit reports, internal investigation findings, and any other resource to help ensure that there is full compliance with the Regulatory Framework, local procedures and any relevant legislation.

Implement the revised controls effectively
Managers must ensure that the revised controls are cost effective and that written procedures are updated informing staff and customers of any changes that affect them. Staff will need to be trained in the use of revised controls and procedures. Managers must also identify any continued weaknesses and adjust as necessary.

Evaluate the effectiveness of controls
Managers should periodically assess the effectiveness of the controls and evaluate whether the risk of fraud has been eliminated or reduced. Advice and support on managing risk, evaluating possible conflicts of interest, or the development or evaluation of controls can be obtained from the Assurance Group.

Any system weaknesses identified as a result of fraud investigations will be reported to the relevant Service Manager, as well as the Head of Assurance, and addressed through an agreed action plan. The relevant Service Manager will be responsible for implementing the action plan. Internal Audit can take on a monitoring role, addressing failures to implement recommendations to the relevant Senior Manager in addition to reporting major system failures, remedial action plans and instances of non-compliance to the Audit & Standards Committee.

Contractors

It is expected that the Council's contractors, and partners, will have adequate controls in place to minimise fraud. We will however raise fraud awareness with our partners as deemed necessary to help them implement robust controls to protect the funds/assets they administer.

Contractors and partners are also expected to have adequate recruitment procedures in place covering requirements under the Immigration and Nationality Act, disclosure & barring checks and stringent vetting in relation to employment history and references. This expectation will form part of all contract terms and conditions.

Employees - Recruitment and Conduct

It is recognised most staff are conscientious and hardworking and whose conduct is beyond reproach. However, where it becomes evident fraud has taken place, action will be taken in accordance with the Council's Disciplinary Rules. Fraud is a specific

instance of gross misconduct and will therefore be treated very seriously. It could involve criminal or civil proceedings as appropriate.
The Council recognises that a key preventative measure is to take effective steps at the recruitment stage to establish, as far as possible, the previous record of potential employees, in terms of their propriety and integrity. Temporary and agency employees will be treated in the same way.

Staff recruitment is required, therefore, to be in accordance with the Council's recruitment and selection policies and written references of potential employees must, wherever practicable, be obtained before employment offers are made. Criminal records will be checked and disclosed prior to appointment in accordance with the Council's Policy.

Employees of the Council are expected to follow the Employees' Code of Conduct and any other Code related to their personal Professional Body.

Employees must comply with their statutory obligations regarding pecuniary interest in Contracts relating to the Council or fees and rewards other than proper remuneration. They are also required to declare any interests which they have that might be seen to conflict with the impartial performance of their duties.

Members (Elected Councillors)

Members are expected to conduct themselves in a way that is beyond reproach, above suspicion and fully accountable by acting in a manner that sets an example to the community they represent and employees who implement their policy objectives.

Members are required to operate within the Council Constitution and Member Code of Conduct with the Standards Committee taking on responsibility of advising and training members relating to these codes. These matters are specifically brought to the attention of Members are also made aware of the declaration and registration of potential areas of conflict between Members' Council duties and responsibilities and any other areas of their personal or professional lives.

Detection and Investigation (to be read alongside the Fraud Response Plan)

While the council has preventative internal control systems which are generally sufficient in themselves to deter fraud, it is often the alertness of employees, Members and the public that enables detection to occur and the appropriate action to take place when there is evidence that fraud may be in progress.

Employees must report any suspected cases of fraud to the appropriate manager, or, if necessary, direct to the Counter Fraud Manager. The Fraud Response Plan appended to this policy provides guidance on what to do when an individual suspects fraud has, or is, taking place.

Reporting cases in this way is essential to the Counter Fraud Policy and makes sure that suspected cases of fraud are investigated properly, a standard process is followed and all connected persons, and the Council's interests, are protected.

The Counter Fraud Team is at the forefront of the Council's fight against fraud and will examine all allegations of theft, fraud and financial malpractice, corruption and behaviour likely to adversely impact on the finances or integrity of the Council, its Members and employees. This extends to allegations against organisations funded by the Council or those with whom the council has a contract and those who receive council services.

It is expected that the Council's partners will provide full and unrestricted access to their financial records relating to the council finances and the co-operation of their staff with any investigation. In addition, personnel records of any person suspected of involvement in fraud against the council will also be made available to the Counter Fraud Team.

Referral to the Police will be undertaken in consultation with the Head of Assurance and in accordance with the Council's Prosecution Policy, alongside any need to obtain further evidence or in cases, such as serious organised crime, where the matter cannot be pursued in house. In cases involving Members, the Standards Committee would determine the issue of Police involvement. Complaints of misconduct under the Members Code of Conduct will be dealt with in accordance with the Standards Committee's arrangements.

Recovery, Sanction and Redress

The strongest available sanctions will be applied to all who commit fraud against the Council, its clients or the public purse. This may include disciplinary action, prosecution and civil proceedings or a combination of all three. Where appropriate to do so, recovery of losses/compensation will be sought and confiscation of proceeds of crime pursued in accordance with relevant legislation. This also applies to employees who defraud or steal from the Council's clients. Disciplinary action will also be taken against staff found to have committed fraud against other Local Authorities, or any other agency administering public funds. The decision regarding sanctions will be taken on a case by case basis having regard to the Disciplinary Rules and Prosecution Policy.

Contractors, or partner organisations, will be expected to take appropriate action against the individual(s) concerned with the ability to request removal of staff considered in contract terms.

Sanctions imposed in relation to cases of fraud involving Members, will be imposed by the Standards Committee in accordance with powers bestowed under appropriate Regulations.

Definitions

What is theft?

Under section 1 of the Theft Act 1968 "A person is guilty of theft if: he dishonestly appropriates property belonging to another with the intention of permanently depriving the other of it."

Examples include stealing property belonging to the council or which has been entrusted to it, such as cash, equipment, vehicles and data as well as stealing property belonging to our staff or members whilst on council premises.

Under section 24A of the Theft Act 1968, a person is also guilty of theft where 'they dishonestly retain a wrongful credit'. For example, where they do not report and repay an overpayment of salary or advance.

What is fraud?

The Fraud Act 2006 introduced the first legal definition of fraud as the intention to make a gain for oneself or another or to cause loss to another/expose another to a risk of loss by dishonestly making a false representation, dishonestly failing to disclose to another person information which he/she is under a legal duty to disclose or occupies a position in which he is expected to safeguard or not to act against the financial interests of another person and dishonestly abuses that position.

Fraudulent acts may arise from:

- Systems Issues - where a process/system exists which is prone to abuse by either employees or members of the public.
- Financial Issues - where individuals or companies have fraudulently obtained money from the Council such as falsification of expense claims, theft of cash and alteration of records to conceal deficiencies, falsification of invoices for payment or failure to account for monies collected.
- Equipment Issues - where Council equipment is used for personal reasons such as the personal use of council vehicles.
- Resource Issues - where there is a misuse of resources such as theft of building materials or working in a private capacity during contracted hours or whilst sick.

What is corruption?

Corruption is defined as the abuse of a position of trust to gain an undue advantage for oneself or another. Corruption can occur in tendering and awarding of contracts, appointment and reward of external consultants, awarding permissions, planning consents and licenses.

What is Bribery?

Bribery is defined as a financial or other advantage that is offered or requested with the intention of inducing or rewarding the improper performance of a relevant function or activity, or with the knowledge or belief that the acceptance of such an advantage would constitute the improper performance of such an activity. This area is covered in greater depth by the Bribery Act Policy.

Further Support & Guidance

If there are any questions about these procedures, the Assurance Group can be contacted on 020 8227 2850, 020 8227 2393, 020 8227 2307, caft@lbbd.gov.uk or by visiting our intranet pages.

Appendix 1 Fraud Response Plan

The London Borough of Barking and Dagenham is committed to developing a culture of honesty and a tough stance against fraud.

The purpose of this document is to demonstrate and set out the procedures to be followed where theft, fraud or corruption is suspected or detected. It is part of the Council's overall Counter Fraud Policy. It therefore applies to all Members (elected Councillors) and all personnel whether staff of the London Borough of Barking and Dagenham, consultants, agency staff or contractors.

It also provides a framework for responding that enables evidence to be gathered and collated in a way which facilitates an informed initial decision and ensures that any evidence gathered will have been lawfully obtained and will be admissible if the matter proceeds to criminal or civil action.

This document is not an investigation procedure for staff. If you suspect fraud it is vital that you follow the guidance in this plan and report your suspicions to the Assurance Group. Neither does this document provide guidance on fraud prevention. It is quite simply a brief guide on "what to do if you become aware of fraud" and tells you how the Council will respond to suspected or actual occurrences of fraud.

Roles & Responsibilities in Respect of Fraud

All staff and Elected Members have duties under the Council's Corporate Governance arrangements to prevent and detect occurrences of fraud and have a responsibility to ensure compliance with relevant legislation in discharging these duties.

The Assurance Group will maintain a log of all reports, detail actions taken, and conclusions reached, and report periodically to Members of the Audit & Standards Committee.

The Assurance Group will ensure a consistent approach to the conduct of any investigations into matters reported and that proper records of each investigation are kept from the outset, including accurate notes of when, where and from whom evidence was obtained, and by whom.

Where a member of staff is to be investigated, the relevant Chief Officer and Departmental Human Resources Officer will be informed. Normally, the member of staff's line manager will also be informed unless this is deemed to be inappropriate given the circumstances of the case.
If a suspicion is reported to a manager, s/he must pass that suspicion on to the Assurance Group immediately. Any delay could compromise subsequent investigations.

What should staff do if they suspect fraud?

Employees are often the first to become aware that there is something seriously wrong within the Council.
If you suspect or become aware of fraud or any other illegal act against the Council, there are several avenues through which your concerns should be reported.

Initially your concerns should be brought to the attention of your line manager. Alternatively, the matter may be raised with the Assurance Group Officers who can advise or discuss the matter informally. You can also report concerns via the Fraud telephone hotline and/or dedicated email address.

If you feel unable to express concerns openly and wish to report concerns in confidence, you may do so in accordance with the Council's Whistleblowing Policy without having to worry about being victimised, discriminated against or disadvantaged in any way as a result.

When you become aware that there may be a problem you should:

- Make an immediate written note of your concerns, details of any telephone or conversations you have heard or documents you have seen, and note the date, time, and names of the people involved. These notes should be signed, timed and dated. Timeliness is important because the longer you delay writing up the notes, the greater the chances of recollections becoming distorted and the case being weakened
- Pass any documents that would normally come into your possession immediately to the Assurance & Counter Fraud Group Officers if this can be done without alerting suspicions; this should include any relevant e mails

You should not:

- Ignore the concerns or be afraid of raising them. You will not suffer recriminations from your employer because of voicing a reasonably held suspicion
- Approach individuals yourself or convey your suspicions to other staff, except those authorised to deal with the matter. There may be an innocent explanation that resolves your concerns. If you have any doubts about who to consult, speak to the Assurance Group Officers first
- Investigate the matter yourself. There are special rules relating to the gathering of evidence for use in criminal cases. Attempts to gather evidence by persons who are unfamiliar with these rules may jeopardise or undermine the case
- Discuss it with anyone else after you have reported your suspicions

What should a member of the public, or partner, do if they suspect fraud?

The Council encourages members of the public who suspect fraud to contact the Assurance Group in the first instance. Suspicions or identified instances of fraud or other wrongdoing against the Council can be reported via a confidential hotline number.

How will allegations of fraud be dealt with by the Council?

The Assurance Group operates independently of other Council services but will pool resources with other stakeholders such as Internal Audit to provide a joined-up approach to prevention, detection, investigation and prosecution of fraud within the council.

When allegations are received from staff or the public the Assurance Group will establish at an early stage the action to be taken by the Council; this may depend on the nature of the allegation. The matters raised may be investigated internally; however, allegations of wrongdoing involving a criminal act may shape the way the investigation is handled and by whom.

Within ten working days of a concern being received, the responsible officer will write to the complainant acknowledging that the concern has been received. Details of the investigation and outcomes will not be divulged due to privacy and data protection concerns.

If it appears that a criminal act has occurred or where there is evidence of fraud, the Police may be invited to become involved in accordance with the Council's Prosecution Policy.

All staff must cooperate fully with any internal enquiry alongside those from the police or other external body.

Where the police are unable to progress a criminal prosecution, e.g. because the burden of proof is insufficient to convince the Crown Prosecution Service to proceed, legal opinion will be sought as to the expediency of civil action particularly in relation to recovering losses.

Alongside any criminal investigation, an internal investigation will be undertaken to:

- Determine the facts
- Consider if the allegation should be dismissed or
- What action should be taken against any staff found culpable
- Consider what action may be taken to recover any losses to the Council which could include civil action
- Identify whether the Council's systems, controls or procedures need to be improved
- If the outcome of an investigation is that a recommendation is made to refer the employee to a disciplinary Hearing, the Assurance Group Officers will advise the appropriate Service Manager and/or Director and liaise with the Human Resources section to determine the next steps.

A fraud log will be completed detailing every action taken during the investigation, this will include the dates and times that each action undertaken was carried out.

How we gather and deal with evidence

The Assurance Group will normally manage investigations and will be responsible for gathering evidence and will seek to establish whether there is any physical evidence

that fraud has occurred and collect such evidence, recording the time and place that the evidence was obtained.

Where there are reasonable grounds for suspicion, the police may become involved at an early stage however the Assurance Group may still undertake part, or all, of the investigation on behalf of the police. All employees MUST co-operate with the investigation process. Failure to co-operate with an investigation constitutes a disciplinary offence.

If appropriate, and in accordance with Human Resources policies and their agreement, suspension of officers will be considered to ensure unfettered progress of investigations. It should be noted that suspension is a neutral act and in no way implies guilt of the officer.

It is important, from the outset, to ensure that evidence is not contaminated, lost or destroyed. Wherever possible original documents should be retained, secured and handled as little as possible. Under no circumstances should they be marked in any way. Computer data must also be secured and should not be viewed by anyone who is not appropriately trained.

All evidence will be obtained lawfully, properly recorded and retained securely in accordance all relevant legislation.

The outcomes of significant internal investigations will be reported to Assurance Board and the Audit & Standards Committee.

Conducting interviews

Interviews will be conducted in a fair and proper manner and in accordance with the Council's Disciplinary Rules. Documentary evidence will be gathered before any interviews are conducted and if it is established there are any witnesses to the events, the Assurance Group will seek to interview and obtain written statements. File notes of all actions and discussions will be maintained. The veracity of the information provided by witnesses and or other evidence documentary or otherwise will determine whether the employee should be interviewed. Where there is a possibility of subsequent criminal action, interviews may be conducted under caution in compliance with relevant legislation.

Closing the investigation

The investigation will be concluded by deciding whether there is a case to answer and by making recommendations as to appropriate action in a written report to the relevant manager and/or Director as well as offering recommendations to systems and procedures where appropriate.

All matters investigated will be dealt with in accordance with the Council's Human Resources Disciplinary Rules and Code of Conduct for employees. Management will seek advice from Human Resources to establish the correct procedure to progress the matter through the Council's disciplinary framework and where, appropriate and in line with policy, referral to a Disciplinary Hearing.

The Fraud Prosecution Policy

June 2019

Date Last Reviewed:	May 2019
Approved by:	Audit & Standards Committee
Date Approved:	TO BE ADDED
Review Date:	June 2020
Document Owner:	Finance Director

The Council's commitment to the Prosecution Policy

The London Borough of Barking & Dagenham is committed to the protection of public funds through its action against fraud and has adopted a tough stance to fraud and wrong doing perpetrated against it. The Council will seek application of the strongest possible sanctions against those found to have perpetrated fraud against it.

What are the aims and requirements of the policy?

The aim of this prosecution policy is to deter fraud against the Council. This policy sets out the range of sanctions that may be applied where fraud and wrongdoing is identified and the circumstances relevant to their application.

Who is governed by this Policy?

This policy applies to council employees, contractors and members of the public found to have committed fraud and other wrongdoing against the Council. Disciplinary action will also be taken against Council employees found to have committed fraud against other local authorities or any other agency administering public funds.

Executive Summary

The London Borough of Barking & Dagenham is committed to the protection of public funds through its action against fraud.

In order to reinforce the deterrence message, where fraud and wrong doing is identified the Council will employ disciplinary action (in the case of Staff), civil action or criminal sanctions or a combination of all three in parallel, in accordance with this policy. All references to fraud in this document include any other type of fraud related offence – fraud, theft, corruption and bribery as defined in the Counter Fraud policy.

Contents

Fraud Prosecution Policy

The London Borough of Barking and Dagenham is committed to preventing fraud wherever possible. All allegations of fraud will be taken seriously.

Where fraud is found to occur, in any form, it will be dealt with rigorously in a controlled manner in accordance with the principles in the Counter Fraud Strategy. It will be investigated fully, and the London Borough of Barking and Dagenham will prosecute all offenders, where appropriate, including Members, employees, contractors and external partners, in accordance with this policy.

This procedure will be operated in conjunction with the London Borough of Barking and Dagenham's disciplinary procedures and all employees will be subject to disciplinary action as well as any prosecution process.

Where there is clear evidence that a fraudulent, or corrupt, act has been committed the following will be considered before a case is considered for prosecution:

- The seriousness of the case
- The level of evidence available
- The level of money or misappropriated assets involved
- Whether the public interest will be served

In assessing a case for prosecution, the following tests will be applied:

- **The Evidential Test:** To ensure sufficiency of evidence to provide a realistic prospect of conviction

- **The Public Interest Test**: To determine whether it would be in the public interest to proceed

A prosecution will usually be pursued unless there are public interest factors against prosecution which clearly outweigh those tending in favour. To pass the public interest test, the Assurance Group will balance carefully and fairly the public interest criteria as detailed in 'The Crown Prosecution Service's Code for Crown Prosecutors 2010' against the seriousness of the offence.

The public interest criterion includes:

- The likely sentence (if convicted)
- Whether the offence was committed as a result of genuine mistake or misunderstanding
- Any previous convictions and the conduct of the defendant

The Council will in most instances prosecute where the fraud perpetrated:

- was not a first offence

- was planned
- was undertaken by an officer in a position of authority or trust and he or she took advantage of this, or
- involved more than one person

The full tests the council will apply in considering a case for prosecution are set out in Appendix 1.

Fraud Sanctions & Redress

With respect to a prima facie case of fraud, an appropriate combination of the following three sanctions may be applied:

- ***Disciplinary Action*** **-** Application of this sanction is normally internal disciplinary action but may involve a referral to the relevant professional organisation from which professional disciplinary action could ensue
- ***Civil Action*** – to recover money, interest and costs where it is cost effective and desirable for the purpose of deterrence, it may be decided that civil redress is the most appropriate course of action. In such instances the council's legal services team will utilise civil law to recover any losses
- ***Criminal Sanction*** - fines, imprisonment, and compensation orders with or without police involvement

Where it is decided that a criminal prosecution is to be pursued, the Assurance Group will brief the most appropriate Chief Officer, however, the option to prosecute may also be determined by the police in some instances.

Managers should not notify the police directly, except in an emergency to prevent further loss, or where it is necessary for the police to examine an area before it is disturbed by staff or members of the public.

In instances where an investigation reveals either;

- numerous cases of fraudulent activity
- significant value, or
- breaches of the employee code of conduct and/or disciplinary rules

The option of pursuing a series of sanctions (parallel sanctions) may be chosen.

The individual or parallel sanctions that are to be applied will be the decision of the Assurance Group following consultation with the Counter Fraud Manager and Legal Services.

In instances where parallel sanctions are applied, for example, internal disciplinary and criminal sanctions, the Assurance Group will carry out an investigation with a view to criminal prosecution, whilst simultaneously conducting an internal investigation under the Disciplinary Procedure.

The Assurance Group will provide evidence to Human Resources in order that an internal investigation and disciplinary hearing can be taken forward with respect to the evidence given. The advantage of this approach is that all appropriate action is taken at the earliest opportunity.

The Council believes fair and effective prosecution is essential in order to protect public funds and deter fraudulent activity.

Irrespective of the sanctions pursued for general fraud, the council will use all measures available to it to recover any money lost due to fraudulent activity.

In respect to criminal redress, this will be sought through the application for a Compensation Order to the Courts. This Order will not only outline the losses sustained by the council through fraud but also the investigation costs.

In respect of Internal Disciplinary, the council has a responsibility, following the outcome of its investigation, to initiate an appropriate procedure aimed at recovering all monies identified as being lost or misappropriated through fraud.

The mechanism by which misappropriated monies are to be repaid will normally be established and agreed prior to any sanction being applied and may be managed through utilisation of procedures such as deduction from salary or debtor invoicing as well as the recovery of losses from pension entitlements where appropriate.

Where the above mechanisms fail to recover any monies owed to the council, following advice from Legal Services, the Assurance Group will consider the option of civil redress.

Civil redress is available to the council in all instances where initial attempts to recover the loss, such as deduction from salary or debtor invoicing, have failed. In such instances, if considered appropriate, Legal Services will make an application either to the Small Claims or County Court - depending on the value to be recovered.

Where other fraudulently obtained assets are found, action under Proceeds of Crime legislation will also be considered utilising Accredited Financial Investigator resources.

Publicity

Assurance & Counter Fraud Group officers will seek to publicise successfully prosecuted cases, with the aim to deter others and thereby to prevent further frauds. The final decision to publicise will rest with the Council's Media & Public Relations Team.

Further Support & Guidance

If there are any questions about these procedures, the Assurance Group can be contacted on 020 8227 2850, 020 8227 2393, 020 8227 2307, caft@lbbd.gov.uk or by visiting our intranet pages.

Appendix 1

Tests the council will apply in considering a case for prosecution:

The Evidential Test

In deciding whether to refer a case for prosecution, the following tests will be considered:

- Is there sufficient evidence for a realistic prospect of a prosecution?
- Can the evidence be used in court?
- Could the evidence be excluded by the court e.g. because of the way it was gathered or the rule about hearsay?
- Is the evidence reliable?
- Is its reliability affected by such factors as the defendant's age, intelligence or level of understanding?
- What explanation has the defendant given? Is the court likely to find it credible in the light of the evidence as a whole?
- Is the witness's background likely to weaken the prosecution case? e.g. does the witness have any motive that may affect his or her attitude to the case?
- Are there any concerns over the accuracy or credibility of a witness?
- How clear is the evidence?
- Has there been any failure in investigation?
- Has there been any failure in administration including delay?

The Public Interest Test

In deciding, the following factors should also be considered:

- Whether a conviction is likely to result in a significant sentence or a nominal penalty
- Whether the offence was committed as a result of genuine mistake or misunderstanding
- Cost effectiveness of taking the case to court
- Any abuse of position or privilege i.e. a member of staff or Councillor
- Whether the claimant is suffering from either significant mental or physical ill health
- Any social factors
- Any voluntary disclosure
- Any previous incidences of fraud
- The evidence shows that the defendant was a ringleader or an organiser of the offence
- There is evidence that the offence was premeditated i.e. the claim was false from inception

- There are grounds for believing that the offence is likely to be continued or repeated, e.g. by a history of recurring conduct
- The offence, although not serious, is widespread in the area where it was committed

This page is intentionally left blank

Money Laundering Policy

June 2019

Date Last Reviewed:	May 2019
Approved by:	Audit & Standards Committee
Date Approved:	TO BE ADDED
Review Date:	June 2020
Document Owner:	Finance Director

The Council's commitment to the Money Laundering Policy

London Borough of Barking & Dagenham, "the Council", takes a tough stance to fraud perpetrated against it and as such will be taking a proactive approach to the prevention, detection and reporting of suspected money laundering incidents.

What are the aims and requirements of the policy?

The policy has the aim to enable suspicious transactions to be recognised and reported to law enforcement agencies to deter and disrupt such practices

Who is governed by this Policy?

The Money Laundering Policy applies to all staff including and not limited to temporary staff, sessional staff and contractors. A failure to comply could be damaging to the finances and reputation of the Council.

Executive Summary

This Money Laundering Policy sets out the Council's commitment to ensuring compliance with the requirements of the Proceeds of Crime Act 2002, the Money Laundering Regulations 2007 & 2012 and Chartered Institute of Public Finance and Accountancy (CIPFA) guidance for Local Authorities on Money Laundering.

Contents

Money Laundering Policy

Our policy is to prevent, wherever possible, the Authority and its staff being exposed to money laundering; to identify the potential areas where it may occur, and to comply with all legal and regulatory requirements, especially regarding the reporting of actual or suspected cases. It is every member of staff's responsibility to be vigilant.

What is Money Laundering?

Money Laundering is the term used for several offences involving the proceeds of crime. It is the process by which the identity of "dirty" money (i.e. the proceeds of crime and the ownership of those proceeds) is changed so that the proceeds appear to originate from legitimate "clean" sources.

Some areas of the Council's activities are thought to be particularly vulnerable to attempts to launder money and it can simply involve receiving payment for goods or services with "dirty" money – usually cash. The legislation includes possessing, or in any way dealing with, or concealing, the proceeds of any crime.

What is the legal definition?

Money Laundering is defined as:

- concealing, disguising, converting, transferring or removing criminal property from England, Wales, Scotland or Northern Ireland
- being involved in an arrangement which a person knows or suspects it facilitates the acquisition, retention, use or control of criminal property
- acquiring, using or possessing criminal property
- when a person knows or suspects that money laundering activity is taking place (or has taken place), or becomes concerned that their involvement in a matter may amount to a prohibited act under the legislation, they must disclose this as soon as practicable or risk prosecution

What is the legislation?

The Proceeds of Crime Act 2002 and the Money Laundering Regulations 2007 & 2012 places specific obligations on persons who are involved in "relevant business". Offences under the Proceeds of Crime Act, and Money Laundering Regulations, can attract penalties of unlimited fines and up to 14 years' imprisonment.

How can suspicious activity be identified?

Employees dealing with transactions which involve income for goods and services, particularly where large refunds may be made, or large amounts of cash are received, will need to consider issues such as:

For new customers:

- is checking their identity proving difficult?
- is the individual reluctant to provide details?
- is there a genuine reason for using the services provided?
- is the customer attempting to introduce intermediaries to either protect their identity or hide their involvement?
- is the customer requesting a large cash transaction?
- is the source of the cash known and reasonable?

For regular and established customers:

- is the transaction reasonable in the context of the service provider's normal business?
- is the size or frequency of the transaction consistent with the normal activities of the customer?
- has the pattern of the transaction changed since the business relationship was established?

What are the areas at risk of Money Laundering?

Where a need is identified, advice will be provided to managers to enable them to provide more targeted training.

Possible examples relating to the Council include:

- Conveyancing, including Housing Right-to-Buy transactions
- Payments in excess of £10,000 towards business rates, business rents, hall hire etc.
- Refunds of large overpayments to accounts such as Council Tax, hire fees etc.
- Suspiciously low tenders

Generally, for the types of transactions the Council is involved with which are at risk in relation to Money Laundering, the risk is mitigated because these transactions will be with large, well-known companies who will be represented by their solicitors who have their own professional duties regarding the Money Laundering Regulations. Conversely, where we have similar transactions with un-represented individuals or bodies this is an area of greater risk and our response will need to reflect this.

Reporting of Money Laundering concerns

Staff should report any suspicions to the Finance Director, Counter Fraud Manager or Financial Investigation Manager as soon as they arise. Suspicions may be reported informally by telephone or email and the responsible officer will seek to establish the facts of the case, investigate the matter fully and determine whether a formal referral to the National Crime Agency (NCA) is appropriate.

Further Support & Guidance

If there are any questions about these procedures, the Assurance Group can be contacted on 020 8227 2850, 020 8227 2393, 020 8227 2307, caft@lbbd.gov.uk or by visiting our intranet pages.

Whistleblowing Policy

June 2019

Date Last Reviewed:	May 2019
Approved by:	Audit & Standards Committee
Date Approved:	TO BE ADDED
Review Date:	June 2020
Document Owner:	Director of Finance

The Councils commitment to the Whistleblowing Policy

This Whistleblowing Policy sets out the Council's commitment to ensuring compliance with the requirements of the Public Interest Disclosure Act 1998 as amended by the Enterprise and Regulatory Reform Act 2013. The council has designated the Monitoring Officer as the Whistleblowing Officer.

What are the aims and requirements of this policy?

The Council wishes to encourage and enable employees and persons providing services on behalf of or to the council to raise serious concerns within the Council rather than overlooking the issue or 'blowing the whistle' outside.

For that reason, this policy has been put in place to make sure that if you want to come forward and raise any concern within the remit of this policy, you can do so with confidence and without having to worry about being victimised, discriminated against or disadvantaged in any way as a result.

Executive Summary

Sometimes employees and those who contract with the council are the first to spot that something is wrong and putting the council and/or its residents at risk but are reluctant to act for fear of not being taken seriously, that their concerns may not be justified or that they may be victimised for speaking out.

Legislation is in place to protect those that raise legitimate concerns in the public interest and in the right way.

This policy sets out the concerns that are dealt with under the whistleblowing procedure, the way in which you may raise concerns and how the Council will respond to those concerns.

Contents

Whistleblowing Policy

It is our policy is to promote a culture of openness and a shared sense of integrity throughout the Council by inviting employees to act responsibly in order to uphold the reputation of the Council and maintain public confidence.

What is whistleblowing?

Whistleblowing is the reporting of suspected, or ongoing, wrongdoing at work.

We are committed to being open, honest and accountable. For this reason, concerns about malpractice and impropriety are taken very seriously. We want you to be able to raise any concerns that the interests of others and the Council (and therefore residents of Barking and Dagenham) are at risk, within the Council rather than overlooking the issue or 'blowing the whistle' outside.

This is because members of staff may be the first to spot anything that is seriously wrong within the council, however, they might not say anything because they think this would be disloyal, or they might be worried that their suspicions are not justified. They may also be worried that they, or someone, else may be victimised.

That is why we have produced this whistleblowing policy to help staff, including agency workers and contractors, to contact us with concerns. This policy has been put in place to make sure that if you want to come forward and raise any concern which you feel relate to illegal, improper or unethical conduct, you can do so with confidence and without having to worry about being victimised, discriminated against or disadvantaged in any way as a result.

Who is covered by this policy?

The whistleblowing policy applies to all staff including those in schools as well as anyone designated as casual, temporary, agency, contractors, consultants, authorised volunteers or work experience. It also covers those working for suppliers/providing services under a contract with the Council where this or an equivalent whistleblowing policy is in force.

To ensure your concern is treated as whistleblowing, you must identify yourself and the policy is in place to encourage this. We will consider anonymous allegations, but it is less likely that we will investigate and achieve a successful outcome.

What types of action are covered by the policy?

The policy is intended to deal with serious or sensitive concerns about wrongdoings that are in the public interest – referred to as public interest disclosures. Your concern may be about members of staff, people who work directly for the Council, suppliers, or people who provide services to the public for us.

When you raise a concern under the whistleblowing policy it must be in the reasonable belief that it is in the public interest to do so. We may ask you to sign a declaration to ensure you understand this principle.

Examples of concerns that may be in the public interest are suspected, or ongoing actions, that fall into the following categories; (the list of actions under each category is not exhaustive)

Criminal Offences

- Misuse of Council funds or Improper or unauthorised use of Council money
- Other fraud or corruption
- Bribery
- An unlawful act
- A person abusing their position for any unauthorised use or for personal gain

Failure to comply with legal obligations

- A person deliberately not keeping to a Council policy, official code of practice or any law or regulation
- A person being discriminated against because of their race, colour, religion, ethnic or national origin, disability, age, sex, sexuality, class or home life

Actions which endanger the health or safety of any individual

- Service users, children or students, particularly children and adults in our care being mistreated or abused
- Any other danger to health and safety

Actions which cause damage to the environment

- The environment being damaged (for example, by pollution)

Actions which are intended to conceal any of the above

- Other wrongdoing including instances where attempts have been made to conceal or cover up wrongdoing

Modern Slavery

- The Modern Slavery Act 2015 was introduced to address concerns about exploitation of people and workers. Modern slavery is a serious form of organised crime in which people are treated as commodities and exploited for criminal gain. Modern slavery, in particular human trafficking, is an international problem. It can take a number of forms, including sexual exploitation, forced labour and domestic servitude, and victims come from all walks of life. The Council, as a responsible public authority, will play its part in elimination of these crimes and so if you have concerns about any organisation or person in contact with the Council who may be involved as a victim or perpetrator please report it right away.

What is not covered by the policy?

You cannot use this policy to deal with serious or sensitive matters that are covered by other procedures, for example:

- Staff complaints about their contract of employment as these are dealt with through our Grievance or Managing Performance at Work procedures.
- Customers' complaints about our services as these are dealt with through our Corporate Complaints Procedure.
- Allegations against Councillors; these should be sent in writing to: Monitoring Officer, Law & Governance, London Borough of Barking and Dagenham, Barking Town Hall, 1 Town Square, Barking IG11 7LU. Write "Private and Confidential" on your envelope. Alternatively, a complaint form and other information is available at: https://www.lbbd.gov.uk/council/councillors-and-committees/councillors/complaints-about-councillors/how-to-complain-about-a-councillor/

You also cannot use this policy to raise issues that have already been settled through other procedures, for example, matters previously resolved under the Council's Disciplinary Rules procedures.

Protecting you

We understand that deciding to blow the whistle is not easy.

When you make a protected disclosure, you have the right not to be dismissed, victimised or subjected to any other detriment. Therefore, we will not tolerate any harassment or victimisation of a whistleblower and will treat such actions as a serious disciplinary offence which will be dealt with under the council Disciplinary Procedure.

We will do our best to protect your identity and keep your concerns confidential if this is what you want.

There may be occasions when you will need to provide statements of evidence for us to conclude the investigation. In this case, we will not reveal your name or position without your permission or unless we must do so by law; for example, if the evidence is required in Court then your anonymity may be subject to the decision of the Courts.

If you work for the Council, you should also know that any allegation you make will not influence, or be influenced by, any unrelated disciplinary action against you or any redundancy procedures that may affect you.

How to raise a concern

The earlier you raise a concern, the easier it will be to take effective action. You should first raise your concern with your immediate Supervisor or Manager (obviously, this will depend on the seriousness and sensitivity of the matter, and who is suspected of the wrongdoing). Alternatively, you may also raise concerns with your Director. Concerns that involve financial malpractice should always be raised with Officers within the Assurance Group.

Please note that any concerns that relate to professionals who:

- Behaved in a way that has harmed a child, or may have harmed a child;
- Possibly committed a criminal offence against or related to a child; or
- Behaved towards a child or children in a way that indicates he or she would pose a risk of harm if they work regularly or closely with children.

Will need to be referred to the Local Authority Designated Officer (LADO) in Children Services: lado@lbbd.gov.uk who will determine if a specific child protection investigation is required.

If you prefer, or you do not work for the Council, you can contact the Assurance Group directly in any of the following ways:

- By writing to the Assurance Group at London Borough of Barking and Dagenham, 2nd Floor Barking Town Hall, 1 Town Hall Square, Barking IG11 7LU (write 'Private and Confidential' on your envelope)
- By phoning the Whistleblowing line on 020 8227 2541. You can leave a confidential voice-mail message 24 hours a day.
- By sending an e-mail to: Whistle.Blowing@lbbd.gov.uk

To maintain confidentiality, you are advised not to copy other people into your message to the whistleblowing mailbox.

If for, whatever reason, you feel your concerns cannot be reported by way of the above reporting options, you can contact the council's Whistleblowing Officer:

- Monitoring Officer, Law & Governance, London Borough of Barking and Dagenham, Barking Town Hall, 1 Town Square, Barking IG11 7LU (write 'Private and Confidential' on your envelope)

If you are putting your concerns in writing it is best to give as much information as possible, such as:

- The reason why you are concerned about a situation
- any relevant names, dates, places and so on
- Background information

- What you personally witnessed or extent to which you have experienced the problem. If possible, you should provide documentary evidence.

You are strongly encouraged to raise your concerns in one of the ways set out above, but if you feel you are unable to raise the matter internally, or feel unsatisfied with any action we take, you could contact our external auditor, BDO London, 55 Baker Street, London, W1U 7EU (020 7486 5888 or www.bdo.co.uk/en-gb/contact) or contact an organisation called Protect (*formerly Public Concern at Work)* for independent advice and support. Protect can be contacted via the following means;

Address:

The Green House
244-254 Cambridge Heath Road
London E2 9DA
Protect Advice Line: 020 3117 2520 (*Option 1)
Protect Advice line: whistle@protect-advice.org.uk

How we respond to your concerns

Within 10 working days of you raising a concern, the Whistleblowing Officer, or designated investigator, will:

- acknowledge that we have received your concern
- explain how we will handle the matter; and
- tell you what support is available to you

It is difficult to set further timescales as they depend on the nature of the allegation and the type of investigation we need to carry out.

The way we deal with the concern will depend on what it involves. If we need to take urgent action, we will do this before carrying out any investigation. We will first make enquiries to decide whether we should carry out an investigation and, if so, how we should go about it. Throughout all our enquiries and any investigation, our main concern will be to put the interests of the public first.

Untrue Allegations

If you make an allegation which you believe is true, but it is not confirmed by our investigation, we will not take any action against you.

However, if the investigatory process finds you have made an allegation which you know is untrue; we will take appropriate disciplinary or legal action against you.

Further Support & Guidance

If there are any questions about these procedures, the Monitoring Officer can be contacted on 020 8227 2114; alternatively, the Assurance Group can be contacted on 020 8227 2850, 020 8227 2393, 020 8227 2307, caft@lbbd.gov.uk or by visiting our intranet pages.

This page is intentionally left blank

The Regulation of Investigatory Powers Act Policy

June 2019

Date Last Reviewed:	May 2019
Approved by:	Audit & Standards Committee
Date Approved:	TO BE ADDED
Review Date:	June 2020
Document Owner:	Finance Director

Purpose

(For text in **bold**, see glossary of terms – Appendix 1)

The RIPA Policy covers the proper conduct of crime prevention activities that involve use of covert **directed surveillance, covert human intelligence sources** or the accessing of **communications data**. Application of the policy ensures that the Council is operating in accordance with the RIPA Act 2000 (the 2000 Act) as amended by the Protection of Freedoms Act 2012 (the 2012 Act). This policy sets out the Council's approach; it details the checks and balances in place to ensure that any use of covert techniques is lawful, necessary and proportionate.

Staff found to have breached the Acts or the Council's Code of Practice are deemed to have breached the Council's Employee Code of Conduct and will be liable to disciplinary action.

Related Documents

The Act must be considered in tandem with associated legislation including the Human Rights Act (HRA) as well as the General Data Protection Regulation **(**GDPR).

Investigations should be conducted in accordance with the Council's Counter Fraud Strategy & Counter Fraud Policy.

Who is Governed by this Policy

The RIPA Policy covers all council staff and those working on behalf of the Council who are engaged in prevention and detection activities which involve the use of surveillance, accessing communications data or use of covert human intelligence sources.

Executive Summary

Regulation of a Local Authority's use of surveillance, use of covert human intelligence sources and accessing of communications data is set out in the RIPA Act 2000 as amended by the Protection of Freedoms Act 2012

Local Authorities' abilities to use these investigation methods are restricted in nature and may only be used for the prevention and detection of serious crime or disorder. Local Authorities are not able to use **intrusive surveillance.** Powers relating to **directed surveillance** were amended by the Protection of Freedoms Act 2012 and the RIPA (Directed Surveillance and CHIS) (Amendment) Order 2012 to limit usage to the purpose of preventing or detecting a criminal offence where the potential punishment is a maximum term of at least 6 months of imprisonment or involving potential offences involving underage sales of tobacco and alcohol.

The RIPA (Communications Data) order came into force in 2004. It allows Local Authorities to acquire **communications data**, namely service data and subscriber

details for limited purposes. This order was updated by The Regulation of Investigatory Powers (Communications Data) Order 2010.

The Act also directs how applications will be made and how, and by whom, they may be approved, reviewed, renewed, cancelled and retained.

The purpose of Part II of the Act is to protect the privacy rights of anyone in a Council's area, but only to the extent that those rights are protected by the Human Rights Act. A public authority such as the Council can infringe those rights, if it does so in accordance with the rules, which are contained within Part II of the Act. Should the public authority not follow the rules, the authority loses the impunity otherwise available to it. This impunity may be a defence to a claim for damages or a complaint to supervisory bodies, or as an answer to a challenge to the admissibility of evidence in a trial.

Further, a Local Authority may only engage the Act when performing its 'core functions'. For example, a Local Authority may rely on the Act when conducting a criminal investigation as this would be considered a 'core function', whereas the disciplining of an employee would be considered a 'non-core' or 'ordinary' function.

In line with the Code of Practice issued by Central Government associated with the 2012 Act, LBBD will only use covert surveillance under RIPA powers where it is proportionate and necessary to do so, and only in the investigation of serious criminal offences.

Contents

Page

Introduction

'It is essential that the Chief Executive, or Head of Paid Service, together with the Directors and the Heads of Units should have an awareness of the basic requirements of RIPA and an understanding of how it might apply to the work of individual council departments. Without this knowledge at senior level, it is unlikely that any authority will be able to develop satisfactory systems to deal with the legislation. Those who need to use, or conduct directed surveillance or CHIS on a regular basis will require more detailed specialised training' (Office of Surveillance Commissioners).

Directed Surveillance

The use of directed surveillance or a CHIS must be necessary and proportionate to the alleged crime or disorder. Usually, it will be a tool of last resort, to be used only when all other less intrusive means have been used or considered.

The Council will conduct its directed surveillance operations in strict compliance with the DPA principles and limit them to the exceptions permitted by the HRA and RIPA, and solely for the purposes of preventing and detecting crime or preventing disorder.

The **Senior Responsible Officer** (SRO) (Appendix 4) will be able to give advice and guidance on this legislation. The SRO will appoint a **RIPA Monitoring Officer** (RMO). The RMO will be responsible for the maintenance of a **central register** that will be available for inspection by the Investigatory Powers Commissioner's Office (IPCO). The format of the central register is set out in Appendix 6.

The use of hand-held cameras and binoculars can greatly assist a directed surveillance operation in public places. However, if they afford the investigator a view into private premises that would not be possible with the naked eye, the surveillance becomes intrusive and is not permitted. Best practice for compliance with evidential rules relating to photographs and video/CCTV footage is contained in Appendix 7. Directed surveillance may be conducted from private premises. If they are used, the applicant must obtain the owner's permission, in writing, before authorisation is given. If a prosecution then ensues, the applicant's line manager must visit the owner to discuss the implications and obtain written authority for the evidence to be used.

This policy does not affect the general usage of the council's CCTV system. However, if cameras are specifically targeted for directed surveillance, a RIPA authorisation must be obtained.

Wherever knowledge of **confidential information** is likely to be acquired or if a vulnerable person or juvenile is to be used as a CHIS, the authorisation must be made by the Chief Executive, who is the Head of Paid Service (or in his absence whoever deputises for them).

Directed surveillance that is carried out in relation to a **legal consultation** on certain premises will be treated as intrusive surveillance, regardless of whether legal privilege applies or not. These premises include prisons, police stations, courts,

tribunals and the premises of a professional legal advisor. Local Authorities are not able to use **intrusive surveillance**. Operations will only be authorised when there is sufficient documented evidence that the alleged crime or disorder exists and when directed surveillance is a necessary and proportionate step to take to secure further evidence.

Low level surveillance, such as 'drive-bys' or everyday activity observed by officers during their normal duties in public places, does not need RIPA authority. If surveillance activity is conducted in immediate response to an unforeseen activity, RIPA authorisation is not required. However, if repeated visits are made for a specific purpose, authorisation may be required. In cases of doubt, legal advice should be taken.

When vehicles are being used for directed surveillance purposes, drivers must always comply with relevant traffic legislation.

Necessary

A person granting an authorisation for directed surveillance must consider *why* it is necessary to use covert surveillance in the investigation *and* believe that the activities to be authorised are necessary on one or more statutory grounds.

Proportionate

The authoriser must also believe the proposed activities are proportionate to what is being sought to be achieved by carrying them out. This involves balancing the seriousness of the intrusion into the privacy of the subject of the operation (or any other person who may be affected) against the need for the activity in investigative and operational terms.

The authorisation will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary. The fact that a suspected offence may be serious will not alone render intrusive actions proportionate. Similarly, an offence may be so minor that any deployment of covert techniques would be disproportionate. No activity should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means.

The following elements of proportionality should therefore be considered:

- balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;
- explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
- considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;
- evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

Crime Threshold

The Regulation of Investigatory Powers (Directed Surveillance and CHIS) (Amendment) Order 2012 imposes a 'Crime Threshold' whereby only crimes which are either punishable by a maximum term of at least 6 months' imprisonment (whether on summary conviction or indictment) or are related to the underage sale of alcohol or tobacco can be investigated under RIPA.

The crime threshold applies only to the authorisation of directed surveillance by local authorities under RIPA, not to the authorisation of local authority use of CHIS or their acquisition of CD. The threshold came into effect on 1 November 2012.

A Local Authority **cannot** authorise directed surveillance for preventing disorder unless this involves a criminal offence(s) punishable (whether on summary conviction or indictment) by a maximum term of at least 6 months' imprisonment.

Thus, LBBD will continue to authorise use of directed surveillance in more serious cases if the other tests are met – i.e. that it is necessary and proportionate and where prior approval from a Magistrate has been granted.

LBBD will also continue to authorise the use of directed surveillance for preventing or detecting specified criminal offences relating to the underage sale of alcohol and tobacco where the necessity and proportionality test is met and prior approval from a Magistrate has been granted.

A local authority **may not authorise** the use of directed surveillance under RIPA to investigate disorder that does not involve criminal offences

An Authorising Officer's Aide-Memoire is provided at Appendix 8 to assist Authorising Officers when considering applications for directed surveillance.

Covert Human Intelligence Sources

A person who reports suspicion of an offence is not a **Covert Human Intelligence Source** (CHIS), nor do they become a CHIS if they are asked if they can provide additional information, e.g. details of the suspect's vehicle or the time that they leave for work. It is only if they establish or maintain a personal **covert relationship** with another person for covertly obtaining or disclosing information that they become a CHIS.

Any consideration on the use of CHIS can only be considered with prior discussion with the Chief Operating officer and/or Director of Law, Governance and Human Resources.

For some test purchases, it will be necessary to use a CHIS who is, or appears to be, under the age of 16 (a juvenile). Written parental consent for the use of a juvenile CHIS must be obtained prior to authorisation, and the duration of such an authorisation is 1 month instead of the usual 12 months. The Authorising Officer must be the Chief Executive or Deputy. **NOTE: A juvenile CHIS may not be used to obtain information about their parent or guardian.**

Officers considering the use of a CHIS under the age of 18, and those authorising such activity must be aware of the additional safeguards identified in The Regulation of Investigatory Powers (Juveniles) Order 2000 and its Code of Practice.

A vulnerable individual should only be authorised to act as a CHIS in the most exceptional circumstances. A vulnerable individual is a person who is, or may need, community care services by reason of mental or other disability, age or illness, and who may not be able to take care of themselves. The Authorising Officer in such cases must be the Chief Executive, who is the Head of Paid Service, or in their absence whoever deputises for them.

Any deployment of a CHIS should consider the safety and welfare of that CHIS. Before authorising the use or conduct of a CHIS, the authorising officer should ensure that an appropriate bespoke risk assessment is carried out to determine the risk to the CHIS of any assignment and the likely consequences should the role of the CHIS become known. This risk assessment must be specific to the case in question. The ongoing security and welfare of the CHIS, after the cancellation of the authorisation, should also be considered at the outset.

A CHIS handler is responsible for bringing to the attention of a CHIS controller any concerns about the personal circumstances of the CHIS, as far as they might affect the validity of the risk assessment, the conduct of the CHIS, and the safety and welfare of the CHIS.

The process for applications and authorisations have similarities to those for directed surveillance, but there are also significant differences, namely that the following arrangements must be in place always in relation to the use of a CHIS:

1. There will be an appropriate officer of the Council who has day-to-day responsibility for dealing with the CHIS, and for the security and welfare of the CHIS

   and

2. There will be a second appropriate officer of the use made of the CHIS, and who will have responsibility for maintaining a record of this use. These records must also include information prescribed by the Regulation of Investigatory Powers (Source Records) Regulations 2000. Any records that disclose the identity of the CHIS must not be available to anyone who does not have a need to access these records.

The Authorisation Process

The processes for applications and authorisations for directed surveillance and CHIS are similar, but note the differences set out in the CHIS section above. Directed Surveillance & CHIS applications are made using forms in Appendix 5.

The authorisation process involves the following steps:

Investigation Officer

1. The Investigation Officer prepares an application. When completing the forms, Investigation Officers must fully set out details of the covert activity for which authorisation is sought to enable the Authorising Officer to make an informed judgment.

2. A risk assessment must be conducted by the Investigation Officer within 7 days of the proposed start date. This assessment will include the number of officers required for the operation; whether the area involved is suitable for directed surveillance; what equipment might be necessary, health and safety concerns and insurance issues. Care must be taken when considering surveillance activity close to schools or in other sensitive areas. If it is necessary to conduct surveillance around school premises, the applicant should inform the head teacher of the nature and duration of the proposed activity, in advance.

3. The Investigation Officer will pass the application through to one of their service's "gatekeepers" for review.

4. The gatekeeper, having reviewed the application, will forward the request to the RIPA Monitoring Officer or another officer within the Assurance Group. The application will be logged on the central register and assigned a unique reference number. The RIPA Monitoring Officer will then submit the application form to an authorising officer (see Appendix 4) for approval.

5. All applications to conduct directed surveillance (other than under urgency provisions – see below) must be made in writing in the approved format.

Authorising Officer (AO)

6. The AO considers the application and if it is considered complete the application is signed off and returned to the Monitoring Officer who will log the outcome within the central register. This process, along with the initial application and dealings with the Monitoring Officer, can be completed through email.

7. An Authorising Officer's Aide-Memoire is provided at Appendix 8 to assist Authorising Officers when considering applications for directed surveillance.

8. If there are any deficiencies in the application further information may be sought from the Investigation Officer, prior to sign off.

9. Once final approval has been received the Investigation Officer will retain a copy and will create an appropriate diary method to ensure that any additional documents are submitted in good time.

Application to Magistrates Court

10. The countersigned application form will form the basis of the application to the Magistrates Court (see further below)

Authorised Activity

11. Authorisation takes effect from the date and time of the approval from the Magistrates Court.

12. Where possible, private vehicles used for directed surveillance purposes should have keeper details blocked by the DVLA.

13. Consideration should be given to notifying the relevant police force intelligence units of the operation.

14. Before directed surveillance, activity commences, the Investigation Officer will brief all those taking part in the operation. The briefing will include details of the roles to be played by each officer, a summary of the alleged offence(s), the name and/or description of the subject of the directed surveillance (if known), a communications check, a plan for discontinuing the operation and an emergency rendezvous point.

15. Evidential notes should be made by all officers engaged in the operation. These documents will be kept in accordance with the appropriate retention guidelines.

16. Where a contractor or external agency is employed to undertake any investigation on behalf of the Council, the Investigation Officer will ensure that any third party is adequately informed of the extent of the authorisation and how they should exercise their duties under that authorisation.

Conclusion of Activities

17. As soon as the authorised activity has concluded the Investigation Officer will complete a Cancellation Form (Appendix 5).

18. Originals of the complete application, any review or renewal & the cancellation forms will be retained with the central register. Should the forms have been completed electronically, the Monitoring Officer will retain all correspondence.

Judiciary Authorisation

Under sections 37 and 38 of the Protection of Freedoms Act 2012 a local authority who wishes to authorise the use of directed surveillance or the use of a CHIS under RIPA will need to obtain an order approving the grant or renewal of an authorisation from a JP (a District Judge or lay magistrate) before it can take effect.

The acquisition of **Communications Data** (CD) by Local Authorities was also required but in June 2019 the process changed. The Home Office transitioned all public authorities from RIPA to IPA and this will impact on the communications data acquisition regime. The IPA introduced independent authorisation of CD requests

through the setting up of the Office for CD Authorisations (OCDA). From June 2019, all CD applications must be authorised by OCDA replacing the need to gain judicial approval.
If the JP is satisfied that the statutory tests have been met and that the use of the technique is necessary and proportionate, he/she will issue an order approving the grant or renewal for the use of the technique as described in the application.

The judicial approval mechanism is in addition to the existing authorisation process under the relevant parts of RIPA as outlined above. The current process of assessing the necessity and proportionality, completing the RIPA authorisation/application form and seeking approval from an authorising officer/designated person will therefore remain the same.

The appropriate officer from LBBD will provide the JP with a copy of the original RIPA authorisation and the supporting documents setting out the case. This forms the basis of the application to the JP and should contain all information that is relied upon.

The original RIPA authorisation should be shown to the JP but also be retained by LBBD so that it is available for inspection by the Commissioners' officers and in the event of any legal challenge or investigations by the Investigatory Powers Tribunal (IPT). The court may also wish to take a copy.

Importantly, the appropriate officer will also need to provide the JP with a partially completed judicial application form.

Although the officer is required to provide a summary of the circumstances of the case on the judicial application form, this is supplementary to and does not replace the need to supply the original RIPA authorisation as well.

The order section of the form will be completed by the JP and will be the official record of the JP's decision. The officer from LBBD will need to obtain judicial approval for all initial RIPA authorisations and renewals and will need to retain a copy of the judicial application form after it has been signed by the JP. There is no requirement for the JP to consider either cancellations or internal reviews.

The authorisation will take effect from the date and time of the JP granting approval and LBBD may proceed to use the techniques approved in that case.

It will be important for each officer seeking authorisation to establish contact with the HM Courts & Tribunals Service (HMCTS) administration at the magistrates' court. HMCTS administration will be the first point of contact for the officer when seeking a Judiciary approval. LBBD will need to inform HMCTS administration as soon as possible to request a hearing for this stage of the authorisation.

On the rare occasions where out of hours' access to a JP is required then it will be for the officer to make local arrangements with the relevant HMCTS legal staff. In these cases, we will need to provide two partially completed judicial application forms so that one can be retained by the JP. They should provide the court with a copy of the signed judicial application form the next working day.

In most emergency situations where the police have power to act, then they can authorise activity under RIPA without prior JP approval. No RIPA authority is required in immediate response to events or situations where it is not reasonably practicable to obtain it (for instance when criminal activity is observed during routine duties and officers conceal themselves to observe what is happening).

Where renewals are timetabled to fall outside of court hours, for example during a holiday period, it is the local authority's responsibility to ensure that the renewal is completed ahead of the deadline. Out of hours' procedures are for emergencies and should not be used because a renewal has not been processed in time.

The hearing is a 'legal proceeding' and therefore our officers will be sworn in and present evidence or provide information as required by the JP. The hearing will be in private and heard by a single JP who will read and consider the RIPA authorisation and the judicial application form. He/she may have questions to clarify points or require additional reassurance on specific points.

The attending officer will need to be able to answer the JP's questions on the policy and practice of conducting covert operations and the detail of the case itself. This does not, however, remove or reduce in any way the duty of the authorising officer to determine whether the tests of necessity and proportionality have been met. Similarly, it does not remove or reduce the need for the forms and supporting papers that the authorising officer has considered, and which are provided to the JP to make the case.

It is not LBBD's policy that legally trained personnel are required to make the case to the JP. The forms and supporting papers must by themselves make the case. It is not enough for the local authority to provide oral evidence where this is not reflected or supported in the papers provided. The JP may note on the form any additional information he or she has received during the hearing but information fundamental to the case should not be submitted in this manner.

If more information is required to determine whether the authorisation has met the tests, then the JP will refuse the authorisation. If an application is refused the local authority should consider whether they can reapply, for example, if there was information to support the application which was available to the local authority, but not included in the papers provided at the hearing.

The JP will record his/her decision on the order section of the judicial application form. HMCTS administration will retain a copy of the local authority RIPA authorisation and the judicial application form. This information will be retained securely. Magistrates' courts are not public authorities for the purposes of the Freedom of Information Act 2000.

LBBD will need to provide a copy of the order to the communications SPOC (Single Point of Contact) for all CD requests. SPOCs must not acquire the CD requested until the JP has signed the order approving the grant.

Authorisation periods

The authorisation will take effect from the date and time of the JP granting approval and LBBD may proceed to use the techniques approved in that case.

A written authorisation (unless renewed or cancelled) will cease to have effect after 3 months. Urgent oral or written authorisations, unless renewed, cease to have effect after 72 hours, beginning with the time when the authorisation was granted.

Renewals should not normally be granted more than seven days before the original expiry date. If the circumstances described in the application alter, the applicant must submit a review document before activity continues.

As soon as the operation has obtained the information needed to prove, or disprove, the allegation, the applicant must submit a cancellation document and the authorised activity must cease.

CHIS authorisations will (unless renewed or cancelled) cease to have effect 12 months from the day on which authorisation took effect, except in the case of juvenile CHIS which will cease to have effect after one month. Urgent oral authorisations or authorisations will unless renewed, cease to have effect after 72 hours.

Telecommunications Data - NAFN

The RIPA (Communications Data) Order 2003 allows Local Authorities to acquire limited information in respect of subscriber details and service data. It does NOT allow Local Authorities to intercept, record or otherwise monitor communications data.

Applications to use this legalisation must be submitted to a Home Office accredited Single Point of Contact (SPOC). The Council uses the services of NAFN (the National Anti-Fraud Network) for this purpose.

Officers may make the application by accessing the NAFN website. The application will first be vetted by NAFN for consistency, before being forwarded by NAFN to the Council's Designated Persons for the purposes of approving the online application. The Council will ensure that Designated Persons receive appropriate training when becoming a Designated Person.

The Council's Designated Persons are presently the Operational Director, Enforcement Services Division and the Director of Public Health. NAFN will inform the Designated Person once the application is ready to be reviewed by the Designated Persons.

The relevant Designated Person will then access the restricted area of the NAFN website, using a special code, to review and approve the application. When approving the application, the Designated Person must be satisfied that the acquiring of the information is necessary and proportionate. Approvals are documented by the Designated Person completing the online document and resubmitting it by following

the steps outlined on the site by NAFN. This online documentation is retained by NAFN who are inspected and audited by the Interception of Communications Commissioner Office.

When submitting an online application, the officer must also inform the relevant Designated Person, in order that they are aware that the NAFN application is pending.

Handling of material and use of material as evidence

Material obtained from properly authorised directed surveillance or a CHIS may be used in other investigations. Arrangements in place for the handling, storage and destruction of material obtained using directed surveillance, a CHIS or the obtaining or disclosure of communications data must ensure compliance with the appropriate data protection requirements and any relevant Corporate Procedures relating to the handling and storage of material.

Where the product of surveillance could be relevant to pending or future proceedings, it should be retained in accordance with established disclosure requirements for a suitable period and subject to review.

Training

Officers conducting directed surveillance operations, using a CHIS or acquiring communications data along with Authorising Officers, the Senior Responsible Officer and the RIPA Monitoring Officer must be suitably qualified or trained.

The Senior Responsible Officer in conjunction with the RIPA Monitoring Officer is responsible for arranging suitable training for those conducting surveillance activity or using a CHIS.

All training will take place at reasonable intervals as determined by the Senior Responsible Officer, but it is envisaged that an update will usually be necessary following legislative or good practice developments.

Surveillance Equipment

All mobile surveillance equipment should be securely held and suitability for use discussed with the Security & Investigations or Assurance Group.

RIPA Record Quality Reviews

To ensure directed surveillance authorisations are being conducted in accordance with Council policy, a system of internal quality assurance has been put in place. The Audit & Select Committee will receive quarterly summaries on the Council's use of RIPA.

The Inspection Process

The Investigatory Powers Commissioner's Office (IPCO) will make periodic inspections during which the inspector will interview a sample of key personnel, examine RIPA and CHIS applications and authorisations, the central register and policy documents. The inspector will also make an evaluation of processes and procedures.

Resources

The latest Codes of Practice for RIPA can be found on the GOV.UK website at:

https://www.gov.uk/government/collections/ripa-codes

Further information can be found on the Investigatory Powers Commissioner's Office website & via the Home Office website:

https://www.ipco.org.uk/

http://www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers/

Relevant Acts:

Regulation of Investigatory Powers Act 2000:
http://www.legislation.gov.uk/ukpga/2000/23/contents

Protection of Freedoms Act 2012:
http://www.legislation.gov.uk/ukpga/2012/9/contents/enacted

Human Rights Act 1998:
http://www.legislation.gov.uk/ukpga/1998/42

General Data Protection Regulation:
https://www.eugdpr.org/eugdpr.org.html

The latest version of the RIPA Policy and our documents can be obtained either by contacting the Assurance Group directly or by visiting our intranet pages

If you have any comments or feedback to do with this document, we would like to hear from you, so please get in touch and email us at the following address:

caft@lbbd.gov.uk

GLOSSARY OF TERMS (For full definitions, refer to the Act)

Central Register
The primary record of RIPA & CHIS applications, reviews, renewals, and cancellations and where original documents are stored.

Collateral intrusion
The likelihood of obtaining private information about someone who is not the subject of the directed surveillance operation.

Communications Data
Information on the communication's origin, destination, route, time, date, size, duration, or type of underlying service but not the content.

Confidential information
This covers confidential journalistic material, matters subject to legal privilege, and information relating to a person (living or dead) relating to their physical or mental health; spiritual counselling or which has been acquired or created in the course of a trade/profession/occupation or for the purposes of any paid/unpaid office.

Covert Human Intelligence Source
A person who establishes or maintains a personal or other relationship for the covert purpose of using such a relationship to obtain information or to provide access to any information to another person or covertly discloses information

Covert relationship
A relationship in which one side is unaware of the purpose for which the relationship is being conducted by the other.

Directed Surveillance
Surveillance carried out in relation to a specific operation which is likely to result in obtaining private information about a person in a way that they are unaware that it is happening.

Intrusive Surveillance
Surveillance which takes place on any residential premises or in any private vehicle. A Local Authority cannot use intrusive surveillance.

Legal Consultation
A consultation between a professional legal adviser and his client or any person representing his client, or a consultation between a professional legal adviser or his client or representative and a medical practitioner made in relation to current or future legal proceedings.

Monitoring Officer (MO)
The Monitoring Officer has the day to day responsibility to maintain a central and up-to-date record of all authorisations (Central Register) and arrange appropriate training.

Residential premises
Any premises occupied by any person as residential or living accommodation, excluding common areas to such premises, e.g. stairwells and communal entrance halls.

Reviewing Officer (RO)
The Head of Legal Services has been designated as the Reviewing Officer. The role is responsible for ensuring an oversight to the RIPA policy, an Authorising Officer as well as counter signatory in cases of non-RIPA applications.

Senior Responsible Officer (SRO)
The SRO is responsible for the integrity of the processes for the Council to ensure compliance when using Directed Surveillance or CHIS.

Service data
Data held by a communications service provider relating to a customer's use of their service, including dates of provision of service; records of activity such as calls made, recorded delivery records and top-ups for pre-paid mobile phones.

Surveillance device
Anything designed or adapted for surveillance purposes.

Appendix 2 of F

The Human Rights Act 1998

Key Articles of Schedule 1 of the Human Rights Act relevant to RIPA:

ARTICLE 6 RIGHT TO A FAIR TRIAL

1. In the determination of his civil rights and obligations or of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law. Judgment shall be pronounced publicly but the press and public may be excluded from all or part of the trial in the interest of morals, public order or national security in a democratic society, where the interests of juveniles or the protection of the private life of the parties so require, or to the extent strictly necessary in the opinion of the court in special circumstances where publicity would prejudice the interests of justice.

2. Everyone charged with a criminal offence shall be presumed innocent until proved guilty according to law.

3. Everyone charged with a criminal offence has the following minimum rights:

   a. to be informed promptly, in a language which he understands and in detail, of the nature and cause of the accusation against him;
   b. to have adequate time and facilities for the preparation of his defence;
   c. to defend himself in person or through legal assistance of his own choosing or, if he has not sufficient means to pay for legal assistance, to be given it free when the interests of justice so require;
   d. to examine or have examined witnesses against him and to obtain the attendance and examination of witnesses on his behalf under the same conditions as witnesses against him;
   e. to have the free assistance of an interpreter if he cannot understand or speak the language used in court.

ARTICLE 8 RIGHT TO RESPECT FOR PRIVATE AND FAMILY LIFE

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

If it is proposed that directed surveillance evidence is to be used in a prosecution, or other form of sanction, the subject of the surveillance should be informed during an interview under caution

Appendix 3 of F

General Data Protection Regulations 2018

The eight principles of the Act relating to the acquisition of personal data need to be observed when using RIPA. To ensure compliance, the information must:

- Be fairly and lawfully obtained and processed
- Be processed for specified purposes only
- Be adequate, relevant and not excessive
- Be accurate
- Not be kept for longer than is necessary
- Be processed in accordance with an individual's rights
- Be secure
- Not be transferred to non-European Economic Area countries without adequate protection.

Under the GDPR, the data protection principles set out the main responsibilities for organisations. Article 5 of the GDPR requires that personal data shall be:

"a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

Article 5(2) requires that: "the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

Key RIPA Officers

Authorisation of RIPA applications where there is a likelihood of obtaining Confidential Information can only be given by the Chief Executive or deputy.

Only the Chief Executive, as Head of Paid Service or their deputy, can authorise the use of a vulnerable person or a juvenile to be used as a Covert Human Intelligence Source.

Principal RIPA Officers

Claire Symonds Senior Responsible Officer (SRO)	Chief Operating Officer & Deputy Chief Executive
Kevin Key RIPA Monitoring Officer (MO)	Counter Fraud Manager: Assurance Group
Fiona Taylor Reviewing Officer (RO)	Director: Law & Governance

Authorising Officers

Chris Naylor	Chief Executive
Claire Symonds	Chief Operating Officer and SRO
Fiona Taylor	Director: Law, Governance & Human Resources and RO
Matthew Cole	Director of Public Health
Authorising Officer (AO)	Operational Director

Appointment of Staff designated as "Gatekeepers"

Name	**Designation**
Theo Lamptey	Service Manager, Public Protection
Simon Scott	Senior Investigator – Assurance Group
Jaiyesh Patel	Senior Investigator – Assurance Group

Appendix 5 of F

Judicial Oversight – LBBD Council's Authorised Applicants

I certify that the following have been appointed under Section 223(1) of the Local Government Act 1972 to appear for the Authority and are approved applicants in accordance with section 223(1) Local Government Act 1972:

List of all staff that have attended and passed the training

Name	**Section**	**Appointed from**
Glen Mark	Food Safety, Enforcement Service	12/12/2016
Meribel Mujih	Private Sector Housing, Regulatory Services	13/12/2016
Rob Harvey	Anti-Social Behaviour	13/12/2016
Nicholas Saunders	Anti-Social Behaviour	13/12/216
Pat Jarman	Assurance & Counter Fraud Group	25/01/2017
Arfan Naseem	CCTV & Security	25/01/2017
Geraldine Bowker	Anti-Social Behaviour	25/01/2017
Cenred Elworthy	Trading standards	25/01/2017
Carolyn Greenaway	Care Management	25/01/2017
Simon Scott	Assurance & Counter Fraud Group	26/01/2017
Vincent Searle	Trading Standards	26/01/2017
Natalie Males	Private Sector Housing, Enforcement Service	26/01/2017
Robert Redmond	Regulatory Services	26/01/2017

In addition; all Gatekeepers have attended training and are approved for the purpose of making applications.

Kevin Key
RIPA Monitoring Officer

Unique Reference Number	

RIPA Application Form

Part II of the Regulation of Investigatory Powers Act 2000

Application for Authorisation for Directed

Surveillance

Public Authority *(including full address)*			
Name of Applicant		**Unit/Branch /Division**	
Full Address			
Contact Details			
Investigation/Operation Name (if applicable)			
Investigating Officer (if a person other than the applicant)			

1. Give name and rank or position of authorising officer in accordance with the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 No. 521. The exact position of the Authorising Officer should be given.
2. Describe the purpose of the specific operation or investigation.
3. Describe in detail the surveillance operation to be authorised and expected duration, including any premises, vehicles or equipment (e.g. camera, binoculars, recorder) that may be used.
4. The identities, where known, of those to be subject of the directed surveillance.
• **Name:** • **Address:** • **DOB:** • **Other information as appropriate:**
5. Explain the information that it is desired to obtain as a result of the directed surveillance.

6. Identify on which grounds the directed surveillance is <u>necessary</u> under Section 28(3) of RIPA. *Delete those that are inapplicable. Ensure that you know which of these grounds you are entitled to rely on (SI 2010 No.521).*
NB: UNDER SECTION 28 OF RIPA, THE ONLY GROUND AVAILABLE TO THE COUNCIL IS: "FOR THE PURPOSE OF PREVENTING OR DETECTING CRIME OR OF PREVENTING DISORDER". **THIS APPLICATION MUST BE REJECTED, IF THIS GROUND IS NOT RELEVANT TO THE PROPOSED SURVEILLANCE.**
7. Explain <u>why</u> this directed surveillance is necessary on the grounds you have identified [Code paragraph 3.3].
8. Supply details of any potential collateral intrusion and why the intrusion is unavoidable. [Bear in mind Code paragraphs 3.8 to 3.11.] **Describe precautions you will take to minimise collateral intrusion.**
9. Explain <u>why</u> this directed surveillance is proportionate to what it seeks to achieve. How intrusive might it be on the subject of surveillance or on others? And why is this intrusion outweighed by the need for surveillance in operational terms or can the evidence be obtained by any other means [Code paragraphs 3.4 to 3.7]?

10. Confidential information [Code paragraphs 4.1 to 4.31]. INDICATE THE LIKELIHOOD OF ACQUIRING ANY CONFIDENTIAL INFORMATION:

11. Applicant's Details			
Name (print)		**Tel No:**	
Grade and Rank or position		**Date**	
Signature			

12. Authorising Officer's Statement. [Spell out the "5 Ws" – Who; What; Where; When; Why and HOW– in this and the following box.]
I hereby authorise directed surveillance defined as follows: [*Why is the surveillance necessary, Whom is the surveillance directed against, Where and When will it take place, What surveillance activity/equipment is sanctioned, How is it to be achieved?]*

13. Explain <u>why</u> you believe the directed surveillance is necessary [Code paragraph 3.3]. **Explain <u>why</u> you believe the directed surveillance to be proportionate to what is sought to be achieved by carrying it out [Code paragraphs 3.4 to 3.7].**

14. (Confidential Information Authorisation.) Supply detail demonstrating compliance with Code paragraphs 4.1 to 4.31.				
Date of first review				
Programme for subsequent reviews of this authorisation: [Code paragraph 3.23]. Only complete this box if review dates after first review are known. If not or inappropriate to set additional review dates then leave blank.				
Name (Print)		**Grade and Rank/Position**		
Signature		**Date and time**		
Expiry date and time [e.g.: authorisation granted on 1 April 20016 - expires on 30 June 2016, 23:59]				

15. Urgent Authorisation [Code paragraph 5.9]: Authorising officer: explain why you considered the case so urgent that an oral instead of a written authorisation was given.				
16. If you are only entitled to act in urgent cases: explain why it was not reasonably practicable for the application to be considered by a fully qualified authorising officer.				
Name (Print)		**Grade and Rank or position**		
Signature		**Date and Time**		
Urgent authorisation Expiry date:		**Expiry time:**		
Remember the 72-hour rule for urgent authorities – check Code of Practice.		e.g. authorisation granted at 5pm on June 1st expires 4.59pm on 4th June		

Unique Reference Number	

RIPA Renewal Form

Part II of the Regulation of Investigatory Powers Act 2000

Renewal of a Directed Surveillance Authorisation

Public Authority *(including full address)*	

Name of Applicant		**Unit/Branch /Division**	
Full Address			
Contact Details			
Investigation/Operation Name (if applicable)			
Renewal Number			

Details of renewal:

1. Renewal numbers and dates of any previous renewals.	
Renewal Number	**Date**

2. Detail any significant changes to the information as listed in the original authorisation as it applies at the time of the renewal.

3. Detail the reasons why it is necessary to continue with the directed surveillance.

4. Detail why the directed surveillance is still proportionate to what it seeks to achieve.

5. Indicate the content and value to the investigation or operation of the information so far obtained by the directed surveillance.

6. Give details of the results of the regular reviews of the investigation or operation.

7. Applicant's Details			
Name (Print)		**Tel No**	
Grade/Rank		**Date**	
Signature			

8. Authorising Officer's Comments. <u>This box must be completed.</u>

9. Authorising Officer's Statement.			
I, [insert name], hereby authorise the renewal of the directed surveillance operation as detailed above. The renewal of this authorisation will last for 3 months unless renewed in writing. This authorisation will be reviewed frequently to assess the need for the authorisation to continue.			
Name (Print)	----------	**Grade / Rank**	----------
Signature	----------	**Date**	----------
Renewal From:	**Time:**	**Date:**	

Date of first review.	
Date of subsequent reviews of this authorisation.	

Unique Reference Number	

RIPA Review Form

Part II of the Regulation of Investigatory Powers Act 2000

Review of a Directed Surveillance authorisation

Public Authority *(including address)*			
Applicant		**Unit/Branch /Division**	
Full Address			
Contact Details			
Operation Name		**Operation Number*** *Filing Ref	
Date of authorisation or last renewal		**Expiry date of authorisation or last renewal**	
		Review Number	

Details of review:

1. Review number and dates of any previous reviews.	
Review Number	

2. Summary of the investigation/operation to date, including what private information has been obtained and the value of the information so far obtained.
3. Detail the reasons why it is necessary to continue with the directed surveillance.
4. Explain how the proposed activity is still proportionate to what it seeks to achieve.
5. Detail any incidents of collateral intrusion and the likelihood of any further incidents of collateral intrusions occurring.
6. Give details of any confidential information acquired or accessed and the likelihood of acquiring confidential information.

7. Applicant's Details

Name (Print)		**Tel No**	
Grade/Rank		**Date**	
Signature			

8. Review Officer's Comments, including whether or not the directed surveillance should continue.

9. Authorising Officer's Statement.			
I, [insert name], hereby agree that the directed surveillance investigation/operation as detailed above [should/should not] continue [until its next review/renewal] [it should be cancelled immediately].			
Name (Print):	----------	**Grade / Rank**	----------
Signature:	----------	**Date:**	----------

10. Date of next review	

Unique Reference Number	

RIPA Cancellation Form

Part II of the Regulation of Investigatory Powers Act 2000

Cancellation of a Directed Surveillance authorisation

Public Authority *(including full address)*	

Name of Applicant		**Unit/Branch/Division**	
Full Address			
Contact Details			
Investigation/Operation Name (if applicable)			

Details of cancellation:

1. Explain the reason(s) for the cancellation of the authorisation:

2. Explain the value of surveillance in the operation:

3. Authorising officer's statement.			
I, [**insert name**], hereby authorise the cancellation of the directed surveillance investigation/operation as detailed above.			
Name (Print)	_____	**Grade**	.....
Signature	_____	**Date**	.....

4. Time and Date of when the authorising officer instructed the surveillance to cease.			
Date:		**Time:**	

5. Authorisation cancelled.	**Date:**	**Time:**

Forms can also be obtained from the Assurance and Counter Fraud Group at: caft@lbbd.gov.uk

Or can be printed of and completed as required from the GOV.UK website at:

RIPA Application for Directed Surveillance

Renewal of a Directed Surveillance Authorisation

Review of a Directed Surveillance Authorisation

Cancellation of a Directed Surveillance Authorisation

Central Register

A central register will be maintained by the RIPA Monitoring Officer. The register will contain details of all RIPA and CHIS applications (whether approved or not) and all reviews, renewals and cancellations.

Each operation will be given a unique reference number (URN) from which the year of the operation may be readily identified.

The register will also contain the following information:

- The name of the applicant
- The name of the subject of the surveillance or CHIS activity (for internal enquiries a pseudonym may be used)
- The date and time that the activity was authorised
- The date and time of any reviews that are to be conducted
- The date and time of any renewals of authorisations
- The date and time of the cancellations of any authorisations

Kept in conjunction with the register will be details of the training and updates delivered to authorising officers, a list of authorising officers, a copy of the RIPA policy and copies of all relevant legislation.

The original of all documents will also be held with the register, which will be available for inspection by the Office of the Surveillance Commissioners.

The register will form the basis of statistical returns of RIPA usage by the Council which are periodically compiled.

Best practice regarding photographic and video evidence

Photographic or video evidence can be used to support the verbal evidence of what the officer conducting surveillance actually saw. There will also be occasions when video footage may be obtained without an officer being present at the scene. However, it is obtained, it must be properly documented and retained in order to ensure evidential continuity. All such material will be disclosable in the event that a prosecution ensues.

Considerations should be given as to how the evidence will eventually be produced. This may require photographs to be developed by an outside laboratory. Arrangements should be made in advance to ensure continuity of evidence at all stages of its production. A new film, tape or memory card should be used for each operation.
If video footage is to be used, start it with a verbal introduction to include day, date, time and place and names of officer's present. Try to include footage of the location, e.g. street name or other landmark so as to place the subject of the surveillance.

A record should be maintained to include the following points:

- Details of the equipment used
- Name of the officer who inserted the film, tape or memory card into the camera
- Details of anyone else to whom the camera may have been passed
- Name of officer removing film, tape or memory card
- Statement to cover the collection, storage and movement of the film, tape or memory card
- Statement from the person who developed or created the material to be used as evidence

As soon as possible the original recording should be copied, and the master retained securely as an exhibit. If the master is a tape, the record protect tab should be removed once the tape has been copied. Do not edit anything from the master. If using tapes, only copy on a machine that is known to be working properly. Failure to do so may result in damage to the master.

Stills may be taken from video. They are a useful addition to the video evidence.

Checklist 6: Compiling an Audit Trail for Digital Images
in the National Policing Improvement Agency's document:
"PRACTICE ADVICE ON POLICE USE OF DIGITAL IMAGES which is available at:

http://library.college.police.uk/docs/acpo/police-use-of-digital-images-2007.pdf

provides a list of what information should be included (with date and time of action) in order to make the evidence admissible.

Authorising Officer's Aide-Memoire

Has the applicant satisfactorily demonstrated proportionality? Court will ask itself should (not could) we have decided this was proportionate. Is there a less intrusive means of obtaining the **same** information? What is the risk – to the authority (loss), to the community of allowing the offence to go un-investigated? What is the potential risk to the subject? What is the least intrusive way of conducting the surveillance? Has the applicant asked for too much? Can it safely be limited? Remember – Don't use a sledge-hammer to crack a nut! YOUR COMMENTS	**Yes**	**No**

Has the applicant satisfactorily demonstrated necessity? What crime is alleged to be being committed? Has the applicant described it in full? Is surveillance necessary for what we are seeking to achieve? Does the activity need to be covert, or could the objectives be achieved overtly? YOUR COMMENTS	**Yes**	**No**

What evidence does applicant expect to gather? Has applicant described: (a) what evidence he/she hopes to gain, and (b) the value of that evidence in relation to THIS enquiry? YOUR COMMENTS	**Yes**	**No**
Is there any likelihood of obtaining confidential information during	**Yes**	**No**

this operation? **If "Yes" operation must be authorised by the Chief Executive or in their absence their deputy.**		

Have any necessary risk assessments been conducted before requesting authorisation? Detail what assessment (if any) was needed in this particular case. In the case of a CHIS authorization an appropriate bespoke risk assessment must be completed.	**Yes**	**No**

When applying for **CHIS** authorisation, have officers been identified to: a) have day to day responsibility for the CHIS (a handler) b) have general oversight of the use of the CHIS (a controller) c) be responsible for retaining relevant CHIS records, including true identity, and the use made of the CHIS.	**Yes**	**No**

Have all conditions necessary for authorisation been met to your satisfaction? GIVE DETAILS	**Yes**	**No**

Do you consider that it is necessary to place limits on the operation? IF YES, GIVE DETAILS (e.g. no. of officers, time, date etc.) and REASONS	**Yes**	**No**

Remember to diarise any review dates and any subsequent action necessary by you and/or applicant. Return copy of completed application to applicant and submit original to the Assurance and Counter Fraud Group. Retain copy.

Open Source

Investigators make much use of the internet to assist with their enquiries. Many of the checks completed could be considered 'open source' that are unlikely to amount to either Directed Surveillance or the use of a CHIS. However, consideration must be had for certain circumstances where RIPA authorisation may be deemed appropriate.

a. Normal Use

When an investigator makes normal checks on the internet, accessing information held within the public domain, on a single occasion, this would be considered acceptable and within the bounds of normal usage. Full records must be kept taking into consideration the expectations of the Criminal Procedure and Investigations Act. Throughout an investigation, it would be appropriate for an investigator to make ***occasional*** further checks. If, on the other hand, it becomes apparent that regular checks are taking place to monitor someone's activities, this may constitute Directed Surveillance.

b. Directed Surveillance

When regular checks of the same pages occur, in order to monitor activity, this may be Directed Surveillance. Should this be happening, consideration should be had for the use of RIPA.

c. Covert Human Intelligence Source

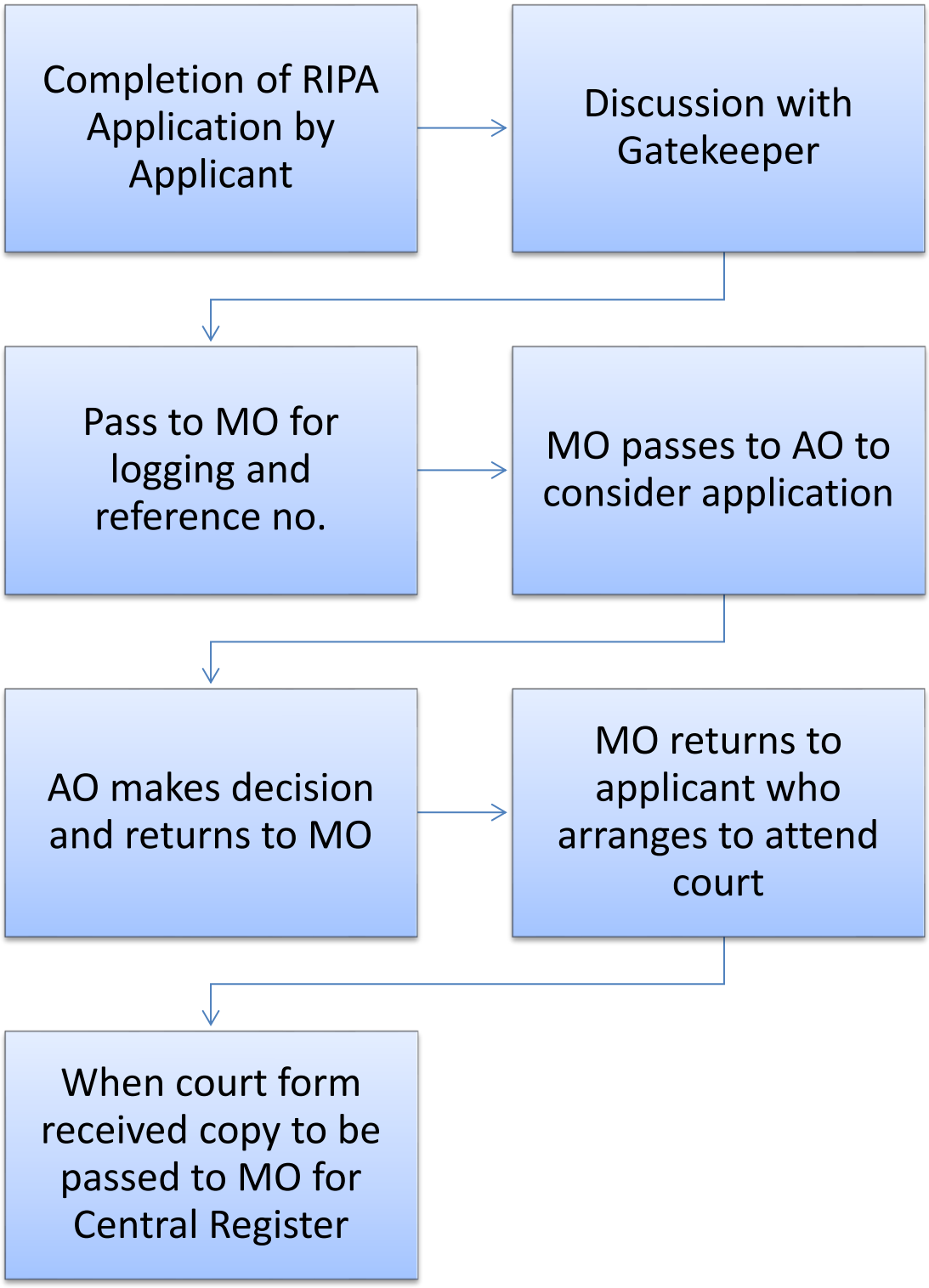
Looking at publicly available pages is considered 'Open Source' but should a decision be made to request access to view page then the situation changes. In order to access specific information a personal or other relationship would have to be created or maintained potentially amounting to the use of a CHIS. An example where this is likely is sending a friend request within Facebook.

EXCEPTION

Should you use an identity that is overt (such as LBBD Fraud Investigations or LBBD trading Standards) to send the request from. In this instance, it would be classed as monitoring and not Directed Surveillance/CHIS.

Officers are encouraged to follow the procedures of this policy (either RIPA or Non-RIPA) should the above circumstances present themselves.

Flow Chart for RIPA Applications



This page is intentionally left blank

The Bribery Act Policy

June 2019

Date Last Reviewed:	May 2019
Approved by:	Audit & Standards Committee
Date Approved:	TO BE ADDED
Review Date:	June 2020
Document Owner:	Finance Director

The Council's commitment to the Bribery Act Policy

The Bribery Act Policy sets out the Council's commitment to ensuring compliance with the requirements of the Bribery Act. The council will not condone acts of bribery, whether it is in the form of money, gifts or a favour, offered or given to a person in a position of trust to influence that person's views or conduct.

What are the aims and requirements of the legislation?

Where Bribery is found to occur, in any form, it will be dealt with rigorously in a controlled manner in accordance with the principles in the Bribery Act policy. It will be investigated fully, and the London Borough of Barking and Dagenham will prosecute all offenders where appropriate including, Members, employees, contractors and external partners.

Who is governed by this Policy?

The Bribery Act policy covers everyone working for us, or on our behalf, including all permanent employees, temporary agency staff, contractors, members of the council (including independent members), volunteers and consultants.

Contents

The Bribery Act Policy

The Bribery Act 2010 makes it an offence to offer, promise or give a bribe (section 1). It also makes it an offence to ask for, agree to receive, or accept a bribe (section 2). Section 6 of the Act creates a separate offence of bribing a foreign public official with the intention of getting or keeping business or an advantage in carrying out business.

There is also a new corporate offence under section 7 of the Bribery Act that we will commit if we fail to prevent bribery that is intended to get or keep business or an advantage in business for our organisation. We are no longer able to claim we were not aware of bribery and may be responsible as an organisation, but we will have a defence if we can show we had adequate procedures in place designed to prevent bribery by our staff or by people associated with our organisation.

Bribery Act policy statement

Bribery is a criminal offence. We do not offer bribes to anyone for any purpose, indirectly or otherwise, and we do not accept bribes. This includes the use of other people, or organisation's, giving bribes to others.

We are committed to preventing and detecting bribery. We take a tough stance against bribery and aim to ensure this Bribery Act policy is observed throughout the Council.

We will deal with allegations of bribery involving employees under our disciplinary procedure as "gross misconduct".

The aim of this policy

This policy provides a framework to allow those affected by it to understand and put into place arrangements to prevent bribery. It will work with related policies, and other documents, to identify and report when this policy is breached and aims to ensure that everyone:

- always acts honestly and protects the council's resources they are responsible for; and
- keeps to the spirit, and letter, of the laws and regulations that cover our work

Scope of this policy

This policy applies to all our activities. All levels of the council are responsible for controlling the risk of bribery and we encourage schools, suppliers and other organisations we work with to adopt policies that are consistent with the principles set out in this policy.

The Bribery Act policy applies to and covers everyone working for us, or on our behalf, including all permanent employees, temporary agency staff, contractors, members of the council (including independent members), volunteers and

consultants. Everyone, at all levels of the council, has a responsibility to control the risk of bribery occurring.

What are "adequate procedures"

For this council to show that we take the Bribery Act seriously, we need to show we have adequate procedures in place designed to prevent bribery. Whether our procedures are adequate will be for the courts to decide. Our procedures need to be in proportion to the level of risk of bribery in our organisation. Individual organisations can refer to six principles to decide whether their procedures are in proportion to the level of risk. These principles are not prescriptive. These principles are intended to be flexible, allowing for the different circumstances of organisations. Small organisations will, for example, face different challenges to those faced by large multi-national organisations. The detail of how an organisation applies these principles will be different depending on the organisation, but the outcome should always be effective Bribery Act procedures.

What are the principles?

1. Proportionate procedures

An organisation's procedures to prevent bribery by the people associated with it should be in proportion to the risks of bribery it faces and to the nature, scale and complexity of the organisation's activities. They should include interrogation of data for the purpose of discovering evidence and ensuring personal data is protected. The procedures should also be clear, practical, accessible and effectively put into place and enforced.

2. Commitment at the top levels of our organisation

Our Cabinet and Senior Management Team are committed to preventing bribery by the people associated with us. They help create a culture in our organisation where bribery is never acceptable.

3. Risk assessment

We regularly assess how and to what extent we will be exposed to potential risks of bribery as part of a wider fraud risk assessment. We keep a record of the assessment, which include financial risks and also other risks such as damage to our reputation.

4. Due diligence

We apply due diligence procedures in relation to people who provide services for or on behalf of our organisation to reduce the risks of bribery. This would include carrying out checks on such organisations or companies and ensuring that they have similar anti bribery processes in place.

5. Communication (including training)

We aim to make sure that our policies and procedures to prevent bribery are understood throughout our organisation. We do this through communication inside and outside of our organisation, including training.

6. Monitoring and review

We monitor and review the procedures designed to prevent bribery and make improvements where they are needed. The Monitoring Officer and Counter Fraud Manager (Assurance Group) will oversee this. We are committed to putting these principles into place as should we be found guilty of an offence under section 7 of the Act, can be fined an unlimited amount.

Facilitation payments
Facilitation payments are unofficial payments made to public officials in order to get them to take certain actions or take actions more quickly. Facilitation payments are illegal under the Bribery Act and we will not tolerate them.

Gifts and hospitality
This policy is in line with our gifts and hospitality policy (this can be read on the Council Intranet). The gifts and hospitality policy make it clear that if members of the council or staff are offered gifts, in their council role, they should not accept anything with more than a token value (examples of things that are of token value include bottles of wine, boxes of chocolates, flowers, pens, calendars and diaries).

Public contracts and failure to prevent bribery
Under the Public Contracts Regulations 2015, persons are to be excluded from consideration to be awarded public contracts if they have been convicted of a corruption offence. Organisations that are convicted of failing to prevent bribery are not automatically barred from competing for public contracts. This is a complex area and procurement advice must be sought where verification has revealed conviction(s) relating to bribery, fraud and other specified unlawful activities within the Regulations. However, we can exclude organisations convicted of this offence from competing for contracts with us. We will include standard clauses in our commercial contracts forbidding bribery and corruption.

Golden Rules

We will not tolerate bribery and those covered by the policy must not:

- give, promise to give, or offer a payment, a gift or hospitality with the expectation or hope that they will receive a business advantage, or to reward a business advantage that they have already been given
- give, promise to give, or offer a payment, a gift or hospitality to a government official or representative to speed up a routine procedure
- accept a payment from another person or organisation if they know or suspect that it is offered with the expectation that it will give them a business advantage
- accept a gift or hospitality from another person or organisation if they know or suspect that it is offered or provided with an expectation that they will provide a business advantage in return
- act against or threaten a person who has refused to commit a bribery offence or who has raised concerns under this policy; or
- take part in activities that break this policy

We are committed to:

- setting out a clear Bribery Act policy and keeping it up to date
- making all employees aware of their responsibility to always keep to this policy
- training employees so that they can recognise and avoid the use of bribery
- encouraging our employees to be aware and to report any suspicions of bribery
- providing our employees with information on suitable ways of telling us about their suspicions and making sure we treat sensitive information appropriately
- investigating alleged bribery and helping the police and other authorities in any prosecution that happens because of the alleged bribery
- taking firm action against any people involved in bribery; and
- including appropriate clauses in contracts to prevent bribery

Employee Responsibilities

All the people who work for us or are under our control are responsible for preventing, detecting and reporting bribery and other forms of corruption. All staff must avoid activities that break this policy and must:

- make sure they read, understand and keep to this policy; and
- tell us as soon as possible if they believe or suspect that someone has broken this policy, or may break this policy in the future

Anyone covered by the policy found to break it will face disciplinary action, potentially leading to dismissal for gross misconduct and/or may also face civil and/or criminal prosecution.

Reporting a concern

We all have a responsibility to help detect, prevent and report instances of bribery. If anyone has a concern about suspected bribery or corruption, they should speak up. The sooner they act, the sooner the situation can be dealt with. There are several ways of informing about any concerns including talking to a line manager first or one of the contacts listed in the Whistleblowing Policy if this is more appropriate.

Those reporting concerns do not have to give us their name. Upon receiving a report about an incident of bribery, corruption or wrong doing, action will be taken as soon as possible to assess the situation. There are clear procedures for investigating fraud and these will be followed in any investigation of this kind. In some circumstances, we will have to consider reporting the matter to the Police or Serious Fraud Office.

Staff that refuse to accept or offer a bribe, or those who report concerns or wrongdoing can understandably be worried about what might happen as a result. To encourage openness and anyone who reports a genuine concern in the public interest will be supported under this policy, even if they turn out to be mistaken. There is a commitment to making sure nobody is treated badly because they have refused to take part in bribery or corruption, or because they have reported a concern.

Further Support & Guidance

If there are any questions about these procedures, the Monitoring Officer can be contacted on 020 8227 2114; alternatively, the Assurance Group can be contacted on 020 8227 2850, 020 8227 2393, 020 8227 2307, caft@lbbd.gov.uk or by visiting our intranet pages.

This page is intentionally left blank

AUDIT & STANDARDS COMMTTEE

3 February 2020

Title: Internal Audit Report 2019/20 Q1 - Q3 (April to December 2019)	
Open Report	**For Decision**
Wards Affected: None	**Key Decision:** No
Report Author: Christopher Martin, Head of Assurance	**Contact Details:** Tel: 020 8227 2174 E-mail: Christopher.Martin@lbbd.gov.uk
Accountable Director: Claire Symonds, Chief Operating Officer	
Summary: This report brings together all aspects of internal audit work undertaken to the end of Q3 of 2019/20. The report details audit progress and results to 31 December 2019 and includes details of the overdue high-risk recommendations outstanding and actions being taken by management to address these.	
Recommendation: The Audit & Standards Committee is asked to note the contents of the report.	

1. Risk and Compliance audits 2019/20

1.1. The Risk and Compliance audit plan has had nine new audits added to the plan since the start of the year with three being removed. These are detailed in section 1 of Appendix 1.

1.2. At the end of Q3, 50% of the original plan of risk and compliance audits were at least at draft report stage. This meets the target for the end of Q3 which is for 50% of audits to be at draft stage.

2. Schools audits 2019/20

2.1. An exercise has been completed to risk assess the schools in the Borough to inform a risk-based schools' audit plan and work is now underway with these schools.

2.2. The 50 days allocated to schools' audits has now been increased to 75 following the risk assessment and this has been split amongst 14 schools and some general follow-up time.

2.3. At the end of Q3, 36% of the school audits were at least at draft report stage. Whilst this does not meet the target for the end of Q3 which is for 50% of school audits to be at draft stage, this is for planned reasons to allow our contractor Mazars to focus on some short notice urgent work on the Risk and Compliance plan.

3. Outcomes of the internal audit work

3.1. Eighteen draft reports have been issued to date, thirteen Risk and Compliance and five School audits. Fourteen final reports (nine Risk and Compliance and five Schools) have also been issued with six of these being Limited Assurance and eight Reasonable Assurance.

4. Progress in implementation of internal audit recommendations as at 31 December 2019

4.1. Internal Audit tracks management progress in implementing all critical and high-risk findings by way of a chase up or follow up to the audit client accordingly.

4.2. There are no outstanding overdue high-risk findings as at 31 December 2019.

4.3. There are no critical findings outstanding.

5. Financial Implications

Implications completed by Thomas Mulloy, Chief Accountant

5.1. Internal Audit is fully funded for 2019/20.

6. Legal Implications

Implications completed by Dr Paul Feild, Senior Governance Solicitor

6.1 The Accounts and Audit (England) Regulations 2015 section require that:

> *a relevant authority must ensure that it has a sound system of internal control which—facilitates the effective exercise of its functions and the achievement of its aims and objectives; ensures that the financial and operational management of the authority is effective; and includes effective arrangements for the management of risk.*

6.2 Furthermore the Director of Finance has a statutory duty, under Section 151 of the Local Government Act 1972 and Section 73 of the Local Government Act 1985, to ensure that there are proper arrangements in place to administer the Council's financial affairs.

6.3 Counter Fraud practices set out in this report address the need to counter fraud, money laundering, bribery and the proceeds of crime. The Councils policies guide on the investigatory and prosecution process. In formulating the policies, it addresses the issue of corruption and bribery. Corruption is the abuse of entrusted power for private gain. The Bribery Act 2010 defines bribery as "the inducement for an action which is illegal, unethical or a breach of trust. Inducements can take the form of gifts, loans, fees, rewards or other advantages whether monetary or otherwise".

6.4 The Local Government Act 1972 provides the Council with the ability to investigate and prosecute offences committed against it. We will enhance our provision further by making best use of existing legislation, for example the Proceeds of Crime Act 2002, to ensure that funds are recovered, where possible by the Council.

Public Background Papers used in the Preparation of the Report: None.

List of Appendices

1 Internal Audit 2019/20 Q3 update

2 Revised Internal Audit Plan 2019/20

This page is intentionally left blank

1. Progress against internal audit plan 2019/20 as at 31 December 2019

Risk and Compliance audits

1.1. The following tables detail the changes to the 2019/20 audit plan made in the period to December 2019:

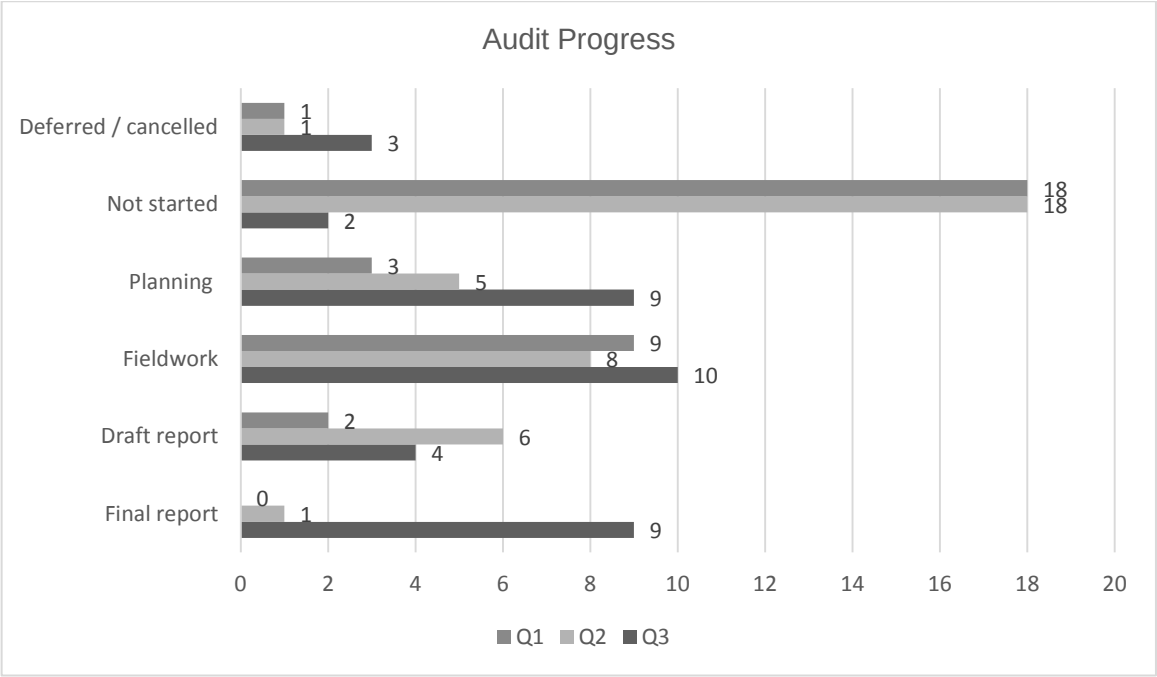
Added	Removed	# of 2019/20 audits as at end of Q3
9	3	**34**

Audit title	Change	Rationale for change
Social Care Forecasting	Added	Management request.
Education, Health and Care Plans	Added	Management request.
Homelessness - Southwark Judgement	Added	Management request.
Capital Programme	Added	Management request.
Right to Buy & Sales Leasing	Added	Management request.
Stewardship of Council Vehicles	Added	Concerns following fraud referral
Data Transparency	Added	Management request
Retrospective Purchase Orders	Added	Issue identified at Procurement Board
Emergency Planning & Business Continuity	Added	To assess improvements in internal control following previous audit
Adaptations Grant Scheme	Deleted	Scheme ceased.
Special Guardianship Orders	Deleted	Assurance gained from other similar audit
Brexit Impact	Deferred	Delay to Brexit process

The current internal audit plan is detailed at Appendix A.

1.2. The table and graph below indicate the progress made against the 2019/20 audit plan as at 31 December 2019.

Not started	Planning	Fieldwork	Draft report	Final report
2	9	10	4	9



School audits

1.3. Historically, schools within the Borough have been audited on a cyclical basis of once every three years using a standard scope and approach for all schools. These audits and the risk assessment had previously been fully outsourced to Mazars.

1.4. This year the Head of Assurance has undertaken his own risk assessment to inform a risk-based approach to schools' audits. The output of this work forms the schools audit plan for 2019/20.

1.5. The following tables detail the changes to the 2019/20 schools audit plan made in the period to December 2019:

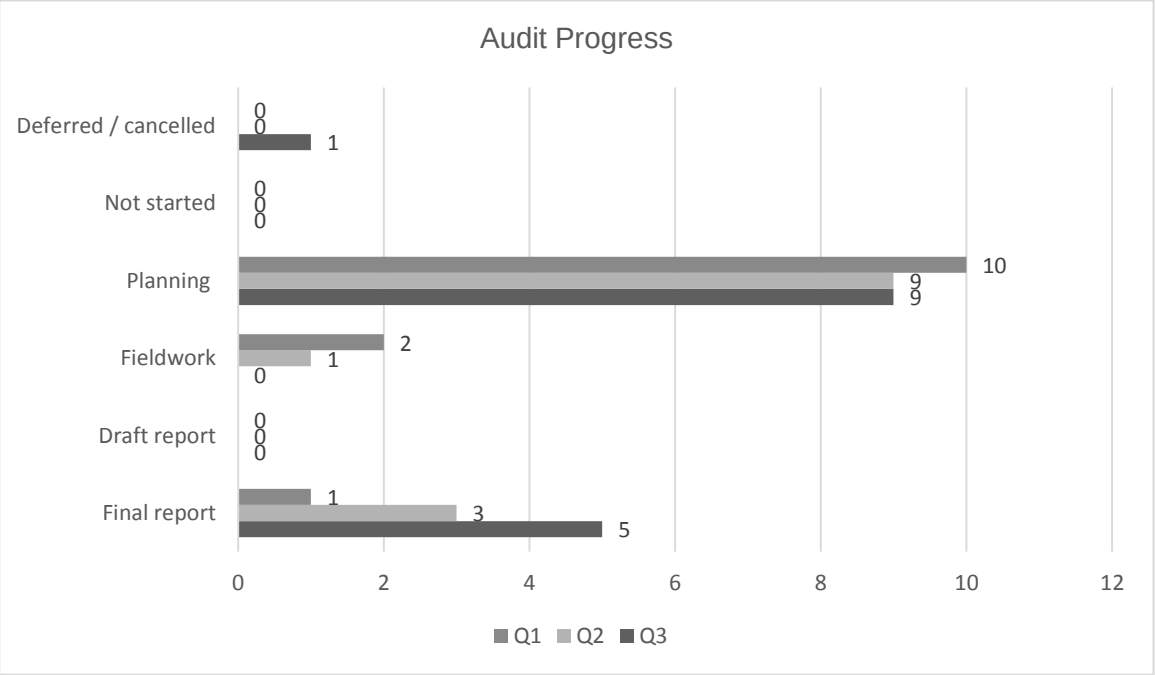
Added	Removed	# of 2019/20 audits as at end of Q3
5	0	**14**

School	Change
All Saints Catholic Secondary	Use of original days
Beam Primary	Use of original days
Becontree Primary	Use of original days
Dagenham Park Secondary	Use of original days
Grafton Primary	Use of original days
Hunters Hall Primary	Use of original days
Jo Richardson Community	Use of original days

Richard Albion Primary	Use of original days
Ripple Primary	Use of original days
School Follow-ups	Use of original days
Robert Clack Secondary	Added
Southwood Primary	Added
Marks Gate Junior	Added
George Carey Primary	Added
Eastbury School	Added

1.6. The table and graph below indicate the progress made against the 2019/20 audit plan as at 31 December 2019.

Not started	Planning	Fieldwork	Draft report	Final report
0	9	0	0	5



2. Progress in implementation of audit findings as at 31 December 2019

2.1. The table below summarises the high-risk findings, as at 31 December 2019, that have reported as final, been implemented, are outstanding and are beyond their due date:

	Reported	Implemented	Outstanding	Beyond due date
2018/19	10	10	0	0
2019/20	15	2	13	0
Total:	**25**	**12**	**13**	**0**

2.2. The current progress in implementing the previously reported overdue high-risk recommendations has been reported by management to be as detailed in the following table:

Finding	Agreed Action	Latest progress
Reported 2018/19		
Asset Management: New Housing Assets and Surveys		
Evaluation of the documented process for the handover of housing assets and adding them to the Housing Asset Register identified the following issues: 1. Timeframes had not been defined for the handover of housing and updating of the housing register. 2. There was no plan for any tracking of houses being received, to ensure that management had sufficient sight of when they were being handed over and that all relevant processes to enable this had been completed. 3. There were no plans to ensure that key stages of the handover process, such as updating the housing asset register, were signed off. 4. Management's process map for the new onboarding process had not been signed off by all of the departments involved. 5. The process map did not include any checks to ensure that only authorised changes were made to the asset register.	The documented process will be developed as follows: 1. Defined target timeframes for handover. 2. Monitoring of performance against the defined timeframes. 3. Tracking of new housing stock, identifying when housing is due to be on boarded and when the key on boarding tasks need to be completed by. 4. Formal sign-off of each stage of new housing handover to evidence completion. 5. Processes required to update the housing records, including defined timeframes and agreed with all relevant business units and the service level directorate. 6. The process to audit a sample of changes to the asset register should be documented. Target 30/06/19	**Implemented December 2019:** My Place have developed and documented a revised process and sign-off form for new build handovers.
Implementation of appropriate controls and processes should prevent or detect key risks to the process objectives.	A timeframe for the implementation of the new handover process will be defined and action owners	**Implemented December 2019:** My Place have developed and documented a revised process and sign-

We were informed by My Place staff that the design of the handover process had not yet been implemented at the time of our audit work in March 2019. We noted that houses were already being received from BeFirst, with 10 properties being onboarded as of the beginning of March 2019. There were no formal processes to ensure that these houses were correctly identified, their condition checked back to the Employer's Requirements or that they were added to the housing register.	set out for each stage. Target 30/06/19	off form for new build handovers.
My Place BDMS Contract Management		
BDMS are the main provider of maintenance services for LBBD housing stock. There are a number of critical services being provided such as repair of boilers in the homes of more vulnerable residents that have to continue even if there is major disruption to the Council or BDMS. Our review of the contract confirmed that it stipulates that BDMS should provide a business continuity plan to ensure that the services can continue in the event of major disruption. However, we identified that this plan had not yet been produced. This meant that there was no documented plan in place to recover these services in the timeframes required by the Council.	A Business Continuity Plan from BDMS will be completed and provided to the Council. The Council will review the BDMS Business Continuity Plan, including reviewing for alignment with the Council's own assessment of the criticality of services. Target: 31/05/19	**Implemented December 2019:** BCP has now been completed and signed off.

3. Internal audit performance as at 31 December 2019

Purpose	Target	Performance & RAG Status	What it measures
Output Indicators (Efficiency)			
% of 2019/20 Audit Plan completed (Audits at draft report stage)	>25% by 30/9/19	26% - GREEN	Delivery measure
	>50% by 31/12/19	45% - AMBER	
	>80% by 31/3/20	N/A	
	100% by 31/5/20	N/A	
Meet standards of Public Sector Internal Audit Standards	Substantial assurance or above from annual review	Confirmed * - GREEN	Compliant with professional standards
Outcome Indicators (Effectiveness - Adding value)			
High Risk Recs not addressed within timescale	<5%	0% - GREEN	Delivery measure
Overall Client Satisfaction	> 85% ratings excellent, good or adequate (i.e. not rated poor)	100% for 2018/19 – GREEN No 2019/20 returns to date.	Customer satisfaction

*Internal Audit for 2019/20 is being provided by a combination of the in-house team, Mazars LLP and PwC LLP. All teams have confirmed ongoing compliance with the Public Sector Internal Audit Standards.

Appendix 2: Revised internal audit plan 2019/20 as at 31 December 2019

1.1. The internal audit plan 2019/20 was approved by the March 2019 Assurance Group and April 2019 Audit and Standards Committee.

1.2. The following audits have occurred or are in progress as at the end of Q3:

Audit title	Audit objective	Status at 31 December 2019
Risk and compliance		
Passenger Transport	As requested, following on from 2018/19 work on Fleet Management	Final report issued in Q2; Limited Assurance
Debt Recovery & Write-offs	Ensuring compliance with financial regulations and that all write-offs are appropriate and necessary and that all debts to LBBD are appropriately chased	Final report issued in Q3; Limited Assurance
Accounts Payable	Key financial – high risk	Final report issued in Q3; Reasonable Assurance
Purchase Cards	Review of controls to ensure that PCs are only used when appropriate and only for bona fide purchases. Recovery of VAT.	Final report issued in Q3; Limited Assurance
Public Health Grant	Review of how the grant is spent, contract managed and delivered	Final report issued in Q3; Reasonable Assurance
Commercial Waste	Audit of control design and operating effectiveness of commercial waste collections	Final report issued in Q3; Reasonable Assurance
KPI Monitoring and Reporting	KPIs are being measured and reported in an accurate, consistent and meaningful manner.	Final report issued in Q3; Limited Assurance
Emergency Planning and Business Continuity	Review of strategic level preparations and how these cascade through the organisation	Final report issued in Q3; Limited Assurance.
Voids	Review of turnaround times and controls in place to minimise void period	Final report issued in Q3; Limited Assurance
Elevate Contract Exit	Deferred from 2018/19. Resources and plans expected to be in place by June 2019. Review of the Council's work preparing for the end of the Elevate contract.	Draft report issued in Q3; awaiting management response
Information Security	How information is gathered, stored, used and disposed of. GDPR compliance	Draft report issued in Q2; awaiting management response
Liquidlogic System Implementation	Deferred from 2018/19 so as not to detract management time from the expected OFSTED inspection. Audit of implementation of the Liquidlogic system in care and support children's and adults	Draft report issued in Q3; awaiting management response
Right to Buy & Sales Leasing	Evaluation of the processes in the Right to Buy and Sales & Leasing team to highlight strengths and weaknesses in internal control.	Draft report issued in Q3; awaiting management response
Procurement	Compliance with Procurement Regulations,	Fieldwork in progress;

Appendix 2: Revised internal audit plan 2019/20 as at 31 December 2019

	ensuring that contracts are in place as appropriate and are being used and that value for money is being achieved. Appropriate use of waivers.	report expected January 2020.
HR On/offboarding	Review of controls surrounding the joiners and leavers process - HR, IT, safeguarding, H&S etc	Fieldwork in progress; report expected February 2020.
Payroll	Key Financial	Fieldwork in progress; report expected January 2020.
Capital Programme	Control design and operation over changes to the Capital Programme including authorisation thresholds with BeFirst	Fieldwork in progress; report expected February 2020.
Management of Heritage Assets	As requested.	Fieldwork in progress; report expected February 2020.
Accounts Receivable	Key Financial	Fieldwork in progress; report expected February 2020.
Freedom of Information Requests	Compliance with regulations and a review of internal process and procedure	Fieldwork in progress; report expected January 2020.
Stewardship of Council Vehicles	Review of controls in place to ensure that the right vehicles are in the right place at the right time and that vehicles are used solely for the business of the Council.	Fieldwork in progress; report expected January 2020.
Data Transparency	A review of the controls in place to ensure that the Council publish information as required and as appropriate.	Fieldwork in progress; report expected February 2020.
Schools		
Risk assessment of schools	Risk assessments of all schools in the borough to inform a risk-based approach to schools' audits.	Completed Q1.
Grafton Primary School	Evaluate the control design and test the operating effectiveness of key controls.	Final report issued Q1 – reasonable assurance
Hunters Hall Primary School	Evaluate the control design and test the operating effectiveness of key controls.	Final report issued Q2 – reasonable assurance
Jo Richardson Community School	Evaluate the control design and test the operating effectiveness of key controls.	Final report issued Q3 – reasonable assurance
Richard Albion Primary School	Evaluate the control design and test the operating effectiveness of key controls.	Final report issued Q3 – reasonable assurance

1.3. The audits planned for the remainder of 2019/20 are set out below. The plan details the draft audit title and draft audit objective:

Audit Title	Audit Objective
Risk and compliance	
Charging Policy	As required

Appendix 2: Revised internal audit plan 2019/20 as at 31 December 2019

Housing System Implementation	Implementation of a new system, involvement from the outset to ensure appropriate controls process established
Mainstay Contract Management	Review of contract monitoring and contract management; pending discussion with service management.
Budgetary Control & Savings Management	Key Financial. Audit of the control design and operating effectiveness of budgetary controls and savings management, including monitoring and reporting of cost savings achieved
Oracle system	Review of key control's around the Council's financial system
Brexit Impact	Review of the Council's assessment of the impact of Brexit and actions planned and taken in response
Private Sector Housing	Deferred from 2018/19. New scheme to be implemented from September 2019.
Education, Health and Care Plans	A review of the operating effectiveness of the relationship between LBBD and BDSIP in this regard.
Social Care Forecasting	Review of key controls around the financial forecasting process.
Homelessness - Southwark Judgement	A review of the treatment of 16 & 17 year olds in the light of the Children Act 1989 and the Housing Act 1996.
Retrospective Purchase Orders	Review of the key causes and remedies of the volume of retrospective purchase orders and non-order payments.
Emergency Planning & Business Continuity	A detailed follow-up of the previous audit work undertaken.
Schools	
School Audits (Q4)	Evaluate the control design and test the operating effectiveness of key controls.: • All Saints Catholic Secondary • Beam Primary • Becontree Primary • Dagenham Park Secondary • Eastbury School • George Carey Primary School • Ripple Primary • Robert Clack Secondary • Southwood Primary • Mark's Gate Junior School

This page is intentionally left blank

AUDIT AND STANDARDS COMMITTEE

3 February 2020

Title: Progress update on External Audit of 2018-19 Accounts	
Report of the Chief Operating Officer	
Open Report	**For Decision**
Wards Affected: None.	**Key Decision:** No
Report Author: Thomas Mulloy, Chief Accountant	**Contact Details:** E-mail: Thomas.Mulloy@lbbd.gov.uk
Accountable Director: Claire Symonds, Chief Operating Officer and S151 Officer	

Summary:

Further to the report to this Committee in July, the Audit of the Council's draft accounts is still ongoing. There have been a notable number of adjustments to the accounts due to misstatements in the draft accounts identified through the testing undertaken by our new external auditors BDO, consequently the audit is taking longer than expected. This is partly due to the complexities of the Council's Group structure, with the Group Accounts consolidating more than 10 subsidiaries.

The Council has, where applicable, accepted amendments to the accounts and, subject to further work, is on track to achieve an unqualified opinion both for the Statement of Accounts and the Value for Money Conclusion.

Recommendation

The Audit and Standards Committee is recommended to delegate authority to the Chief Operating Officer, in consultation with the Chair, to make any material changes to the draft accounts that may be agreed with the Council's external auditor and to complete the sign off process.

Reason(s)

It is a statutory obligation for the Council's Statement of Accounts to be produced and audited in accordance with the timetable as set out in the Audit and Accounts Regulations 2015, and that the Statement of Accounts and the Annual Governance Statement must be approved by a Committee of the Council.

1. Introduction and Background

1.1 The draft Statement of Accounts 2018-19 was approved by the Audit and Standards Committee on 28 July of this year. The external audit of the accounts is still ongoing and all parties involved endeavour to have the audit completed as soon as is practically possible.

2. Audit of Accounts

2.1 Following certification by the Chief Operating Officer by the 31st May 2019 the draft accounts have been subject to detailed and rigorous review by the Council's external auditors, BDO. The audit is still being completed.

2.2 During the audit of the main statements, there have been a significant number of amendments made to the Group Accounts. It is the first year the Council has produced a set of Group Accounts consolidating several subsidiaries. Given there have also been adjustments to the subsidiaries' accounts, including a prior period adjustment in the Be First accounts, these are being reflected in the revised Group Accounts.

2.3 BDO will provide the Committee with an update setting out their current position in regards to the external audit of the accounts at this meeting.

2.4 The Council, along with BDO, will endeavour to complete the audit as soon as possible. Though it should be noted that although there may be a delay there is currently no suggestion that the accounts will be qualified and the Council is aiming for an unqualified opinion, hence the time taken to get the accounts right.

2.5 The Committee's workplan for this meeting had included an item on preparation for the 19/20 audit. As the current audit is still ongoing, this work has not been completed, but conversations have been had with BDO to start to develop a realistic and resourced plan for the coming year with an agreed and achievable time line.

3. Pension Fund

3.1 BDO audit work on the Pension Fund is complete, although as the Pension Fund Accounts form part of the Council's Statement of Accounts, it will not be concluded until the main accounts' audit is also complete. There are no significant issues from the Pension Fund Accounts audit to report, the detailed results of this audit were presented to the last meeting of this Committee.

4. Value for Money Conclusion

4.1 Work by BDO on the Value for Money Conclusion is ongoing and the conclusion cannot be finalised until the main accounts audit is complete. A further update by BDO will be made at the Committee but again there is no indication that this will not be unqualified.

5. Audit of Council's Subsidiaries

5.1 The External Audit (also BDO) of BDSIP, Be First and BDTP has been completed and the accounts have been filed with the Companies House. All were given a clean bill of health by BDO (unmodified opinion). Both Reside entities and B&D Energy Ltd are expected to follow by end of this month.

6. Publication of the Statement of Accounts

6.1 Once BDO provide their formal opinion on the accounts and gives the certificate of closure for the audit, the accounts will then be placed on the Council's website.

7. Financial Implications

7.1 These have been addressed in the body of the report.

8. Legal Implications

8.1 The Local Audit and Accountability Act 2014 (the '2014 Act') requires that the Council as a relevant body must have its accounts audited. The procedure is set out in the Accounts and Audit Regulations 2015 (the 'Regulations). Regulation 9 sets out a timetable and requires certification by the Council's responsible finance officer of the statement and then consideration by a committee to consider the statement and approve by resolution.

Public Background Papers used in the Preparation of the Report: None

List of appendices: None.

This page is intentionally left blank

AUDIT &STANDARDS COMMITTEE

3 February 2020

Title: Corporate Risk Register Update	
Open Report	**For Discussion & Agreement**
Wards Affected: None	**Key Decision:** No
Report Author: Christopher Martin, Head of Assurance	**Contact Details:** Tel: (020) 8227 2174 E-mail: Christopher.Martin@lbbd.gov.uk
Accountable Strategic Leadership Director: Claire Symonds, Chief Operating Officer	
Summary: This report provides an update on the Corporate Risk Register.	
Recommendation: The Committee is asked to note the contents of the report.	

1 Background

1.1. It is essential that robust, integrated systems are developed and maintained for identifying and evaluating all significant strategic and operational risks to the Council. This should include the proactive participation of all those associated with planning and delivering services.

1.2. Risk management is concerned with evaluating the measures in place, and the actions needed, to identify and control risks effectively. The objectives are to secure the Council's assets and to ensure the Council's continued financial and organisational wellbeing.

1.3. Risk offers both significant potential positive and negative impacts on delivery and reputation and it therefore follows that a key organisational challenge facing the Council is embedding risk as part of the organisation's decision making process both in day to day operational situations and at the strategic level.

2. Risk Management

2.1. The LBBD Risk Management vision is that the Council will have a robust system of risk management in place to identify, assess and manage the key risks in the Borough that may prevent it achieving the priorities identified in the Corporate Plan. Effective risk management is a key management tool for LBBD that is used to understand and optimise the benefits it can generate from calculated risk taking, as well as helping to avoid and manage unwanted surprises.

2.2. This report provides an update on how strategic risk continues to be monitored and managed. Details of the process are set out in the LBBD Risk Management Approach which was approved by Cabinet on 17th September 2019 and is appended to this report as Appendix 1.

2.3. The Council's approach to corporate risk management is to embed risk ownership across the organisation so that it is the responsibility of all managers and teams to manage risk. The Council's Head of Assurance is responsible for Risk Management strategy, advice and support but is not responsible for managing risks.

2.4. Directors and Heads of Service ensure that risks within their area are recorded and managed appropriately, in line with the risk management framework. Assurance Group regularly review and monitor the approach to risk management.

2.5. Risk Registers will form part of the service plans and are designed to be dynamic documents, being updated regularly. The Corporate Risk Register covers risks which affect our ability to achieve long-term Council objectives. Risks can be escalated from service risks up to the Assurance Group for inclusion in the Corporate Risk Register or moved down as required. Risks within the Corporate Risk Register state the cause, *event* and **consequence**. For example, "as a result of bad weather, there is a risk that *staff will not be able to get to the office* and undertake their work which will result in **unhappy service users and increased complaints**."

3. Corporate Risks

3.1. The Senior Leadership Team have reviewed all their current key risks to achieving the Council's objectives. This section provides a summary of progress being made in moving towards the desirable level of risk for each entry in the Corporate Risk Register.

3.2. Each Risk Owner has assessed their risk for the following:

- Gross Risk (the impact and likelihood of the risk with no controls in place);
- Net Risk (the impact and likelihood of the risk with current controls in place); and
- Target Risk (the impact and likelihood of the risk, once all further actions have been implemented).

3.3. There are 14 Corporate Risks with results as follows:

1. Population Change - An inability to understand how the population of Barking and Dagenham is changing and developing, could mean LBBD does not having the required social infrastructure to meet the needs of its community, resulting in unsatisfied residents and reputational damage.

Gross Risk	Net Risk	Target Risk

2. Financial Management - Unrealistic financial modelling of grant or company income and benefits may lead to the Authority's funding model no longer being sufficient, resulting in an inability to provide key services and severe reputational damage.

Gross Risk	Net Risk	Target Risk

3. Significant Incident in the Community - A significant incident in the local community, in the context of the current high level of community tensions or a major public catastrophe, may lead to an eruption of civil disobedience, resulting in harm to residents, significant damage to council property, financial loss and a loss of confidence in the council.

Gross Risk	Net Risk	Target Risk

4. Safeguarding Failures - Staff not properly following safeguarding processes, for example due to the pressure of high caseload levels, could ultimately result in the death or serious injury of a child or vulnerable adult, resulting in loss of public faith, reputational damage, high financial costs and challenge and scrutiny from governing bodies.

Gross Risk	Net Risk	Target Risk

5. Development of the Third Sector - A small Third sector may mean the Authority is unable to sufficiently reduce demand for its own services, leading to unsatisfied residents, increased costs and ultimately a failure to meet performance targets.

Gross Risk	Net Risk	Target Risk

6. Investment Decisions - A high number of investment decisions requiring quick turnarounds, coupled with a constraint on the level of relevant skills and resources to properly review these, could lead to inappropriate investment decisions being made, resulting in both financial and reputational damage, in addition to affecting the progress of developments to the council's physical infrastructure.

Gross Risk	Net Risk	Target Risk

7. Economic Downturn - A large shock to the UK economy or a significant economic downturn could impact the Authority's ability to obtain the ambitious financial returns it requires from its wholly owned companies (such as BeFirst), leading to constraints on its available funding.

Gross Risk	Net Risk	Target Risk

8. Contract Management - The current lack of resources and skills in the Authority to manage its major contracts may mean that the contracts do not deliver on the agreed objectives, leading to a failure to deliver services to residents and significant financial loss.

Gross Risk	Net Risk	Target Risk

9. Information Security - A data handling error by a member of staff or a contractor, could lead to the exposure of a substantial amount of residents' information to unauthorised individuals, resulting in significant reputational damage, investigations by the ICO and other bodies and potential fines.

Gross Risk	Net Risk	Target Risk

10. Recruitment & Retention of Staff - A lack of perceived investment in staff and wider remuneration, due to increasing financial pressure on the Authority, may make it difficult to recruit and retain sufficiently. This may be more likely at Director and senior management level, as well as hard to recruit roles. This potentially could lead to impacts on service delivery, financial costs if roles have to be covered by interims and could lead to a significant loss of knowledge within the Authority.

Gross Risk	Net Risk	Target Risk

11. Vision & Cultural Change - LBBD's leadership not clearly articulating the benefits of the current strategy and required transformation as detailed in the Corporate Plan, could lead to pressure from Councillors or residents to adjust the Authority's priorities and objectives, which may lead to sub-optimal allocation of resources and a failure to meet performance targets as well as staff not making the required cultural changes, resulting in the council being unable to deliver on its priorities.

Gross Risk	Net Risk	Target Risk

12. Data Centre Failure - A catastrophic failure of the data centre where LBBD's data is stored could prohibit the Authority from carrying out its day-to-day operations, resulting in residents not receiving services, significant financial implications and severe reputational damage.

Gross Risk	Net Risk	Target Risk

13. Brexit - Rapid population change, acute deprivation and inequality of outcomes compared to the rest of London, in addition to the Borough supporting Leave in the referendum, could lead to significant resident dissatisfaction if the final outcome of Brexit is not in line with resident expectations, resulting in increasing community tensions and potentially increasing the demand for services if it leads to an economic downturn.

Gross Risk	Net Risk	Target Risk

14. Damage to Physical Assets - A significant incident within Barking and Dagenham, such as a major fire or terrorist incident, may lead to damage to the Authority's physical assets, resulting in incident management and repair costs, temporary loss of services and inconvenience to residents.

Gross Risk	Net Risk	Target Risk

3.4 All Risk Owners are provided with a 'Risk on a Page' template to record their risk, controls and actions. Each of these is attached at Appendix 1.

4. Financial Implications

Implications completed by: Katherine Heffernan, Group Manager - Finance

4.1. Risk Management is an integral part of good management and should be embedded in the day to day work of all Council officers and managers and delivered within existing resources. In addition, there are specific fully funded posts within the Finance service that support this work. There are no further financial implications arising from this report.

5. Legal Implications

Implications completed by: Dr Paul Feild, Senior Governance Solicitor

5.1. To reiterate the main body text of this report, risk management is a key role for the organisation across the board for Members, Chief Officers and the teams. As an example, local authorities have a specific leadership role to plan for, be prepared and able to take action to respond to an emergency under the Civil Contingencies Act 2004.

5.2. Furthermore, if a risk is identified and reasonable measures are not taken to mitigate its likelihood of occurrence and if it is preventable, such as for example a tree on the highway was dangerously leaning over, the Council should take action and cut it down before it causes harm. To fail to do so could lead to legal liability to pay compensation for negligence and the reputational damage in not having taken steps to reduce the risk of occurrence and the magnitude of an event. To carry out risk assessments and to devise and implement risk occurrences, elimination and mitigation is therefore a core activity for management.

Public Background Papers Used in the Preparation of the Report: None.

List of Appendices

Appendix 1 Risk Management Approach

This page is intentionally left blank

Appendix 1

Risk Management Approach

September 2019

One borough; one community; no one left behind

London Borough of Barking & Dagenham

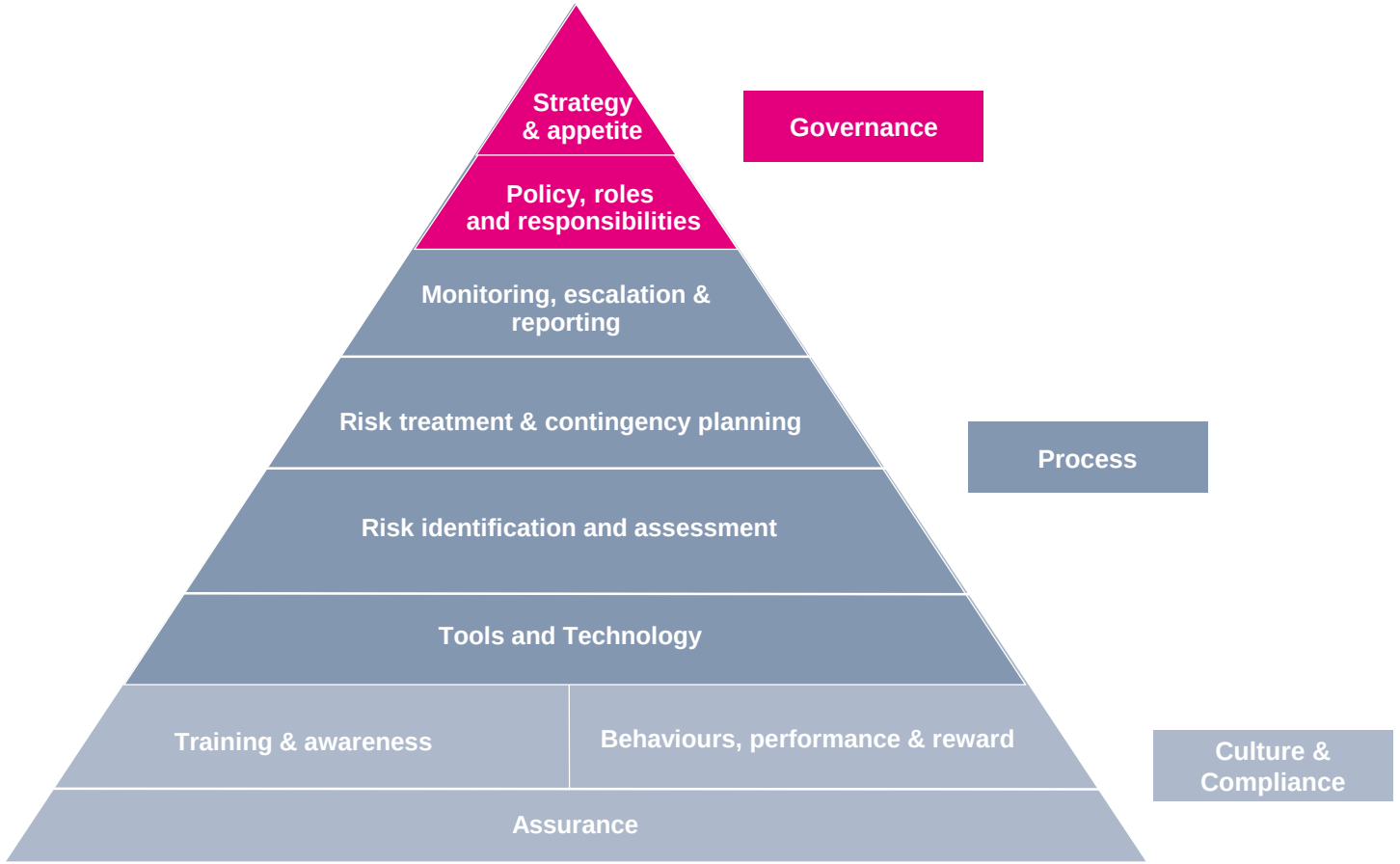
lbbd.gov.uk

Vision

LBBD will have a robust system of risk management in place to identify, assess and manage the key risks in the Borough that may prevent it achieving the priorities identified in the Corporate Plan. Effective risk management will be a key management tool for LBBD, that is used to understand and optimise the benefits it can generate from calculated risk taking, as well as helping to avoid and manage unwanted surprises.

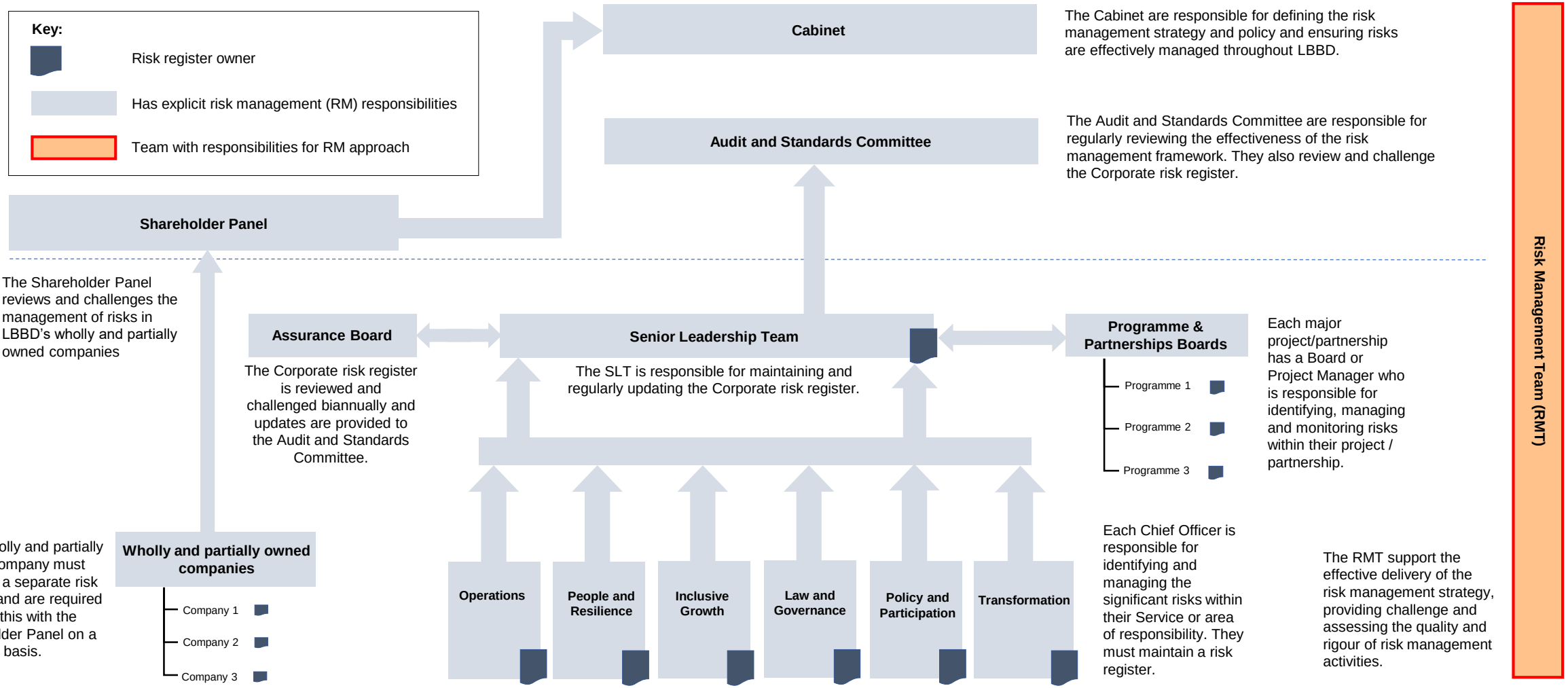
Risk Management Framework

The risk management framework below comprises governance, process, culture and compliance activities. A combination of all these elements is required to enable risk management to operate in an effective and consistent manner throughout LBBD.



Governance

Governance diagram



Key roles and responsibilities

To successfully embed risk management throughout LBBD, the risk management process is supported by a number of defined key roles and responsibilities at each level of LBBD.

Who	Key roles & responsibilities
Cabinet	• Have ultimate accountability to ensure that risks are managed effectively throughout LBBD by maintaining effective systems of risk management and internal control. • Approve the Authority's risk management strategy and policy.
Audit and Standards Committee	• Provide oversight of the effectiveness of the risk management system and assurance activities. • Assist the Cabinet in fulfilling its oversight, challenge and monitoring responsibilities for the integrity, scope and design of the LBBD systems of internal controls and risk management. • Review and challenge the Corporate risk register.
Shareholder Panel	• Reviews and challenges the management of risks in LBBD's wholly and partially owned companies on a quarterly basis.
Assurance Board	• Reviews and challenges the Corporate risk register biannually and provide updates to the Audit and Standards Committee. • Discuss, scrutinise and challenge the approach to managing risk at an officer level. • Responsible for designing and updating the risk management framework and policy. • Receive notification of any material breaches of risk limits or procedures and agree proposed action.
Senior Leadership Team	• Responsible for maintaining and regularly updating the Corporate risk register. • Set the risk appetite for LBBD. • Identify emerging risk areas that warrant focus (e.g. geo-political, regulatory shifts, etc.).
Risk Management Team	• Provide local guidance and support on the risk management framework. • Provide quarterly updates on Chief Officers' risk registers to SLT. • Monitor all red and amber risks and escalating to the SLT if necessary. • Offer consistent independent 'challenge' throughout the process of risk identification, assessment and response and provide their views of the impact and likelihood of risks occurring and the effectiveness of existing controls. • Provide feedback on the overall quality and rigour of risk identification and management activities to individuals and leadership and support continuous improvement.

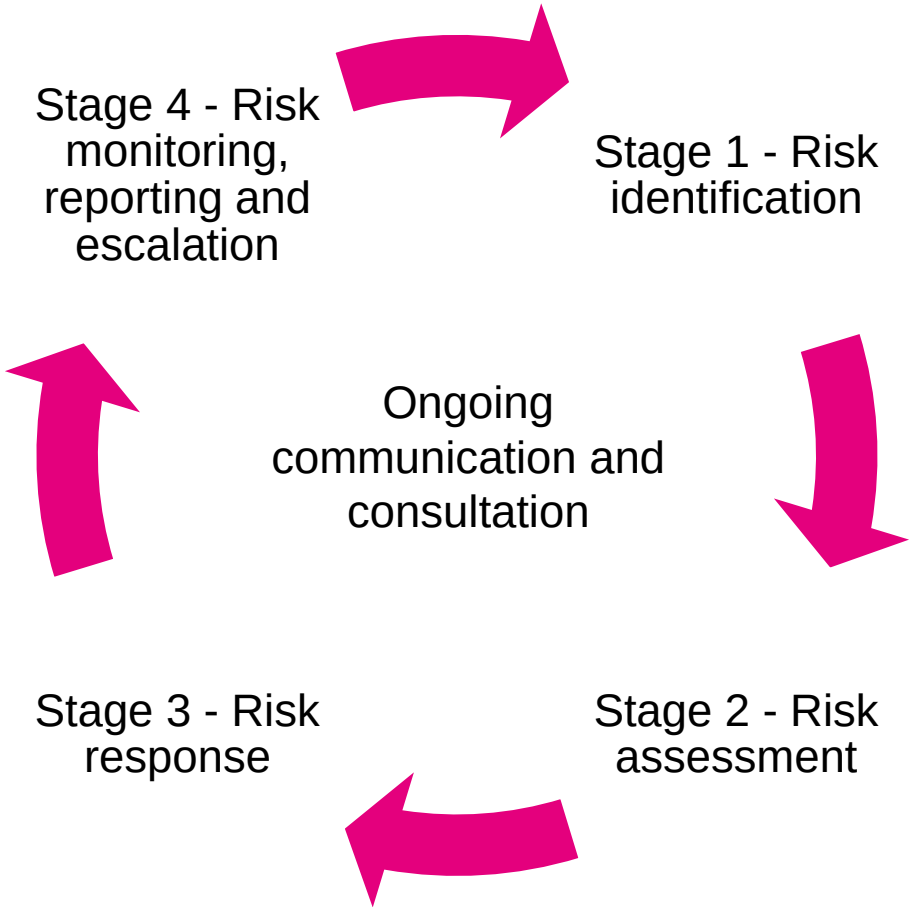
Key roles and responsibilities

Who	Key roles & responsibilities
Chief Operating Officer	• Responsible for the Authority's risk management policy statement and promoting it throughout LBBD.
Chief Officers	• Responsible for identifying and managing the significant risks within their Service or area of responsibility and maintaining a risk register. • Monitor and escalate their identified risks, in line with reporting requirements. • Responsible for implementing the LBBD Risk Management policy within their areas of responsibility. • Support and sponsorship of risk management in their area of responsibility. • Provide the Risk Management Team with quarterly updates of their risks.
Other directors and managers	• Responsible for the identification, management and monitoring of risks within their area.
Wholly and partially owned companies	• Each wholly and partially owned company must maintain a separate risk register and are required to share this with the Shareholder Panel on a quarterly basis.
Risk Management Champions	• Risk Management Champions support their Director with risk management. • Coordinate and support the risk management process in their respective area. • Report the key risk information on a quarterly basis to the Risk Management Team. • Provide day-to-day support and advice on the risk management policy and process to management and staff. • Liaise with the Risk Management Team to ensure that good practice risk management activities are shared across LBBD.
Risk Owners	• Specific risk owners, e.g. CFO / DCS / DAS. • This is a named individual with allocated ownership for each risk identified, who has single point of accountability and responsibility for the effective management of the risk. • Be familiar with the risk and have the required authority to ensure its effective management. • Be responsible for assessing and agreeing the severity of the risk and it's mitigation plan. • Be accountable for monitoring the risk to identify any material changes or issues.
Programme & Partnership Boards or Project Managers	• Responsible for the identification, management and monitoring of risks within their project/partnership.

Risk Management Process

Risk management process

The risk management process is comprised of four main stages and is applicable across the whole of LBBD. The key activities and requirements for each stage of the risk management process are detailed below.



- Establish the context and environment (e.g. the team involved and the scope of their area)
- Identify and describe all key risks to achieving priorities, using 'cause, event, consequence' structure
- Allocate a single risk owner for each risk who has overall accountability for the management of the risk
- Capture risks in risk register template

- Apply the LBBD assessment criteria to the assessment of all risks
- Assess all risks on an Inherent, Net and Target basis

- Take further action if a difference is identified between Net and Target score
- Select risk treatment: Avoidance, Reduction, Transfer or Acceptance

- Capture and report risk information on a timely basis
- Escalate risks in line with criteria
- Risk owners to monitor their risks on a regular basis

Stage 1 – Risk identification

1) Establish the context and environment of the risk (i.e. the scope of the area involved and the internal and external factors affecting the current environment).
2) Use the risk identification timeline to define the period over which risks should be identified.
3) Clearly identify risks in terms of 'cause, event and consequence'.
4) Assign each risk an individual risk owner.

1) What is a risk?

A risk:

- is forward-looking (not a current issue)
- has an element of uncertainty
- could affect the achievement of priorities
- must be credible and foreseeable
- could lead to positive or negative effects

2) Risk identification timeline

Defining the time period during which a risk could materialise is important as it will influence which risks are identified, how they are assessed and how the mitigation activities are prioritised. LBBD risks should be considered in the context of occurrence within a five-year period.

3) Describing a risk

Cause - The source of the risk event, the reason why the risk could happen

Event - Actions, incidents, or occurrences that arise from a cause that could have an effect on the achievement of priorities

Consequence(s) - Effects arising from the risk event, if it occurs, that could affect the achievement of priorities

Example of a risk description

"Insolvency of key supplier X, could lead to an inability to provide the required level of critical security services in the Borough for over 4 weeks, resulting in increased costs of [£], potential serious injuries to staff and residents and potential legal claims from residents of over [£]."

This risk description is precise and clearly identifies a single cause, the risk event and the consequences of the risk materialising. By identifying a specific cause, the risk can be accurately assessed, and effective controls can be put in place to manage the risk.

Stage 2 – Risk assessment

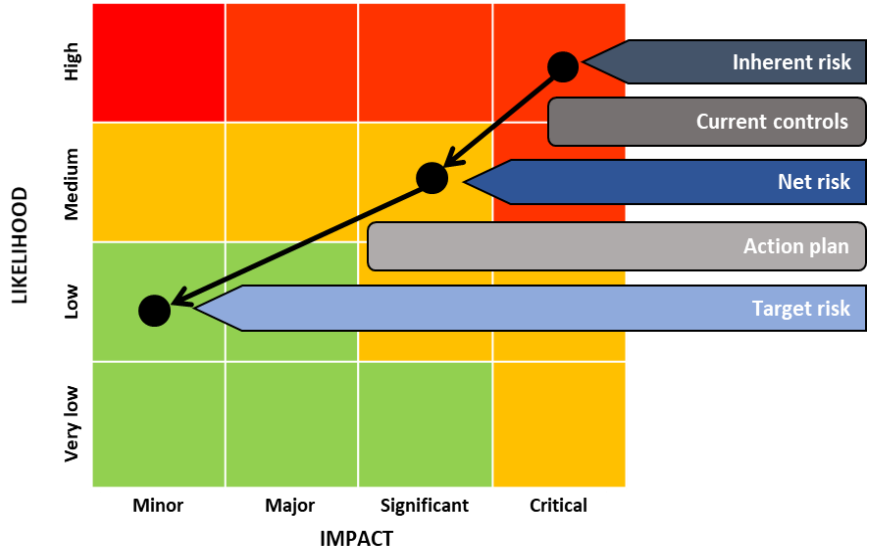
Assess the risk by considering two factors: the likelihood of the risk materialising and the potential impact(s) of the risk if it were to occur.

Likelihood - The likelihood of a risk occurring is determined by estimating the probability of the risk occurring within a five-year period.

Impact - The impact of a risk is established by considering its potential effects on the achievement of LBBD's priorities.

Risks should be assessed on three different basis:

Inherent	Net	Target
The impact and likelihood of the risk with no controls in place.	The impact and likelihood of the risk with current controls in place.	The impact and likelihood of the risk, once all further actions have been implemented.



Stage 2 – Risk assessment - Impact criteria

The impact of a risk is established by considering its potential effects on the achievement of LBBD's strategic priorities. A standard scale to score a risk's effects is used. The impact is measured against four levels of severity using the impact factors detailed below. Where multiple impact areas are applicable, the assessment should be based on the factor with the highest impact.

Factor	Operational	Reputational	Health, Safety & Environment	Legal/ Regulatory	Financial	Effect on Project Objectives/ Scheduled Deadlines
Critical	A key service cannot be delivered to the majority of residents for more than 7 days Failure of a strategic partnership Unauthorised release of constituents' personal data to a third party, including sensitive details	Prolonged, high profile national media coverage of over 7 days Adverse central government response that involves removal of delegated powers Officer(s) and/or Members forced to resign &/or governing body enquiry	Fatality(s) or permanent disabilities/illness to service users Fatality(s) or permanent disabilities/illness to employees or councillors Government / regulator / HSE investigation and action leads to restrictions on Authority providing a key service	Litigation / claims / fines costing £250k+ Statutory prosecution	Costing over £500,000 Up to 50% of Budget	Completion of a major project is delayed for 3 months or more
Significant	A key service cannot be delivered to the majority of residents for 2-7 days Failure of an operational partnership Unauthorised release of constituents' personal data to a third party, not including sensitive details	High profile national media coverage for 3-7 days	Multiple RIDDOR (Reporting of Injuries, Diseases and Dangerous Occurrences Regulations) injuries to employees or councillors	Litigation / claims / fines costing £100k to £250k	Costing between £50,000 and £500,000 Up to 25% of Budget	Completion of a major project is delayed for 2-3 months

Stage 2 – Risk assessment - Impact criteria

Factor	Operational	Reputational	Health, Safety & Environment	Legal/ Regulatory	Financial	Effect on Project Objectives/ Scheduled Deadlines
Major	A key service cannot be delivered to the majority of residents for 1-2 days	High-profile media coverage within Greater London for more than 7 days	RIDDOR injury/illness to employees or councillors Significant deterioration of Council owned buildings, historical assets reducing the aesthetic amenity of an area.	Litigation / claims / fines costing £50k to £100k	Costing between £5,000 and £50,000 Up to 10% of Budget	Completion of a major project is delayed for 3-8 weeks
Minor	A key service cannot be delivered to the majority of residents for less than 1 day	High-profile media coverage within Greater London for 3-7 days	Non-RIDDOR injury/illness that results in lost time to employees or councillors	Litigation / claims / fines costing £25k to £50k	Costing less than £5,000 Up to 5% of Budget	Completion of a major project is delayed for less than 2 weeks

Stage 2 – Risk assessment - Likelihood criteria

The likelihood of a risk should be considered in the context of occurrence at LBBD within a five-year period.

Likelihood	% of occurrence
High	>80%
Medium	50 - 80%
Low	20 - 50%
Very Low	≥20%

Stage 2 – Risk assessment - Example

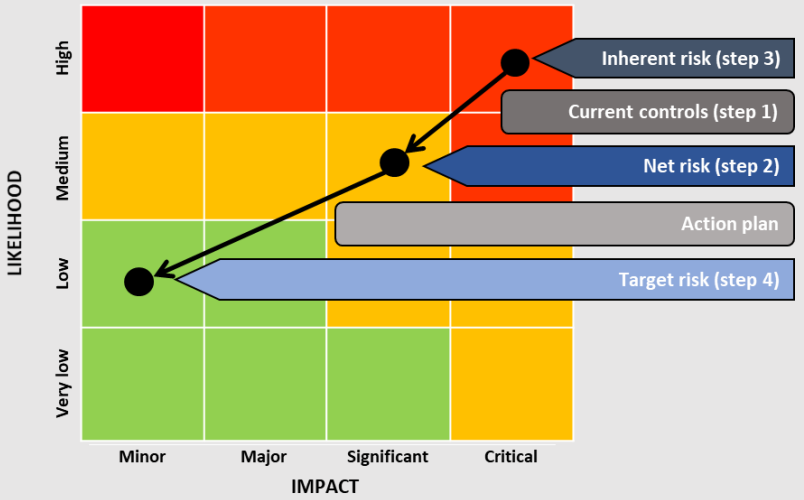
Risk description: *"Insolvency of key supplier X, could lead to an inability to provide the required level of critical security services in the Borough for over 4 weeks, resulting in increased costs of [£], potential serious injuries to staff and residents and potential legal claims from residents of over [£]."*

Step 1 – Current controls

Identify all significant controls that have an effect on actively managing the risk and consider their effectiveness. Focus on the identification of controls that are specifically in place to manage the risk (reducing its likelihood or impact) and have a material effect on its management.

Controls for the example risk description:

- *Supplier due diligence process, including assessment of suppliers' financial stability*
- *Potential insolvency notification requirement in all supplier contracts*
- *Supplier Failure insurance*



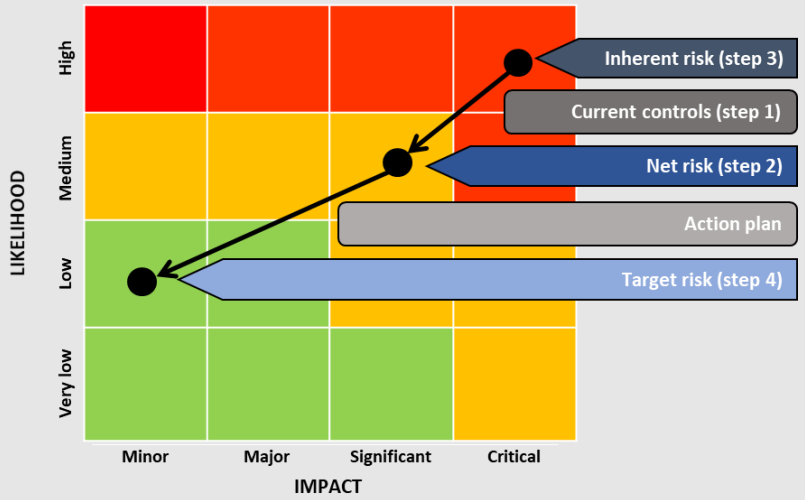
Step 2 – Assess the Net position

Taking account of controls, estimate the Net risk score. Given the effectiveness of the controls in place, what is the risk score (likelihood and impact of the risk) now?

Based on the described risk and its controls, and using LBBD's risk assessment criteria, in this example the Net risk position is assessed to have an impact of Critical and a likelihood of Medium.

Stage 2 – Risk assessment - Example

Risk description: *"Insolvency of key supplier X, could lead to an inability to provide the required level of critical security services in the Borough for over 4 weeks, resulting in increased costs of [£], potential serious injuries to staff and residents and potential legal claims from residents of over [£]."*



Step 3 - Assess the Inherent position

Estimate what the impact and likelihood of the described risk would be if all the current controls (identified in Step 1) did not exist.

In this example, the Inherent risk position is assessed to have an impact rating of Catastrophic and likelihood rating of High.

Step 4 – Assess the Target position

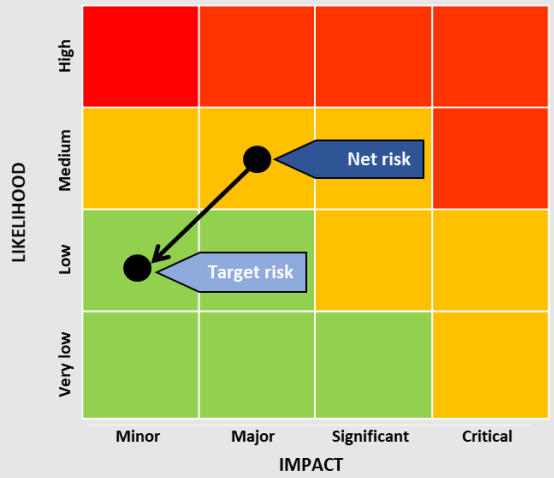
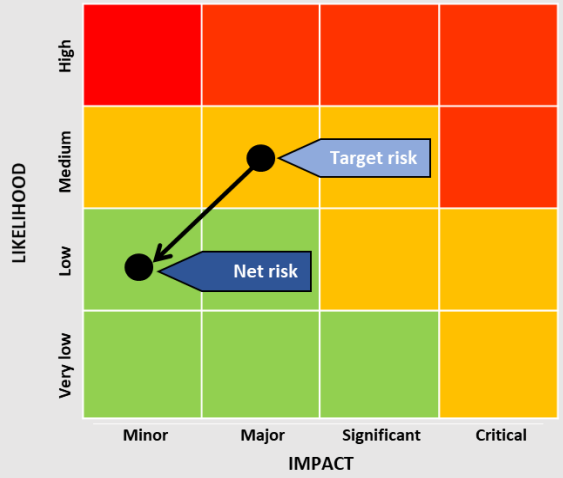
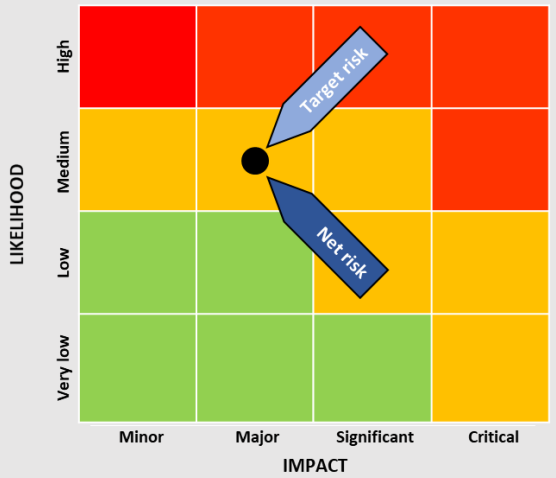
Consider whether the current Net risk position is acceptable or whether the realistic desired impact and likelihood values are different.

In this example, the Target Risk is set at an impact rating of Marginal and a likelihood rating of Low. Considering the Net risk position, the impact and likelihood is determined not to be acceptable. The acceptable position is lower, and therefore requires further response activities to be put in place. For the example risk, these could include, for example, the roll-out of predictive indicators for key suppliers (such as monitoring supplier requests for improvements in payment terms, significant price increases and reductions in on-time delivery rates) and reducing the reliance on a key supplier by moving to several smaller suppliers.

Stage 3 – Risk treatment - types of action required

Once the Target risk position has been established, it should be compared against the Net risk position to understand if a risk response is required.

There are three possible outcomes:

a) The Net risk score is greater than the Target risk score	b) The Net risk score is less than the Target risk score	c) The Net risk score is the same as the Target risk score
		
Action required: Reduce the level of risk exposure to an acceptable level by developing and implementing further mitigating actions that will reduce the Net risk exposure to the Target position.	**Action required:** Consider relaxing or removing controls until risk exposure is aligned with Target position. This can realise cost savings on existing responses and/or allow greater reward for taking more risk.	**No further action required:** Maintain and monitor controls to confirm that they remain effective. No action plan required.

Stage 3 – Risk treatment

Where the Net risk score is greater than the Target score ((a) on previous page), implement appropriate action(s) to bring the Net risk score in-line with the Target.

The risk owner has overall accountability for the management of the risk, though action owners can be assigned to implement specific response activities. There may be a number of response options available; these should be considered by the risk owner, based on the evaluation of their effectiveness, cost and feasibility.

Risk response options can be grouped as follows:

Avoidance	**Exiting the activities that give rise to risk, as the risk is unacceptable:** • Avoiding or eliminating the risk by deciding not to start or continue with the activity that gives rise to the risk, or by doing something differently e.g. substitution of an alternative step or activity. • This can reduce the risk to zero but may introduce other risks as a result that need to be evaluated.
Reduction	**Action taken to reduce risk impact and/or likelihood:** • Decreasing the likelihood and/or impact through enhancing existing controls or implementing additional controls.
Transfer	**Reducing risk likelihood or impact by transferring or otherwise sharing a portion of the risk:** • Common techniques include outsourcing activities or purchasing insurance products (Note: transferring does not necessarily eliminate or remove accountability or the effects of the risk e.g. outsourcing a process may not reduce the reputational impact to LBBD if something goes wrong but may reduce the likelihood if the third party is better placed to manage the risk).
Acceptance	**No action is taken to affect risk impact or likelihood. This means the current risk exposure is accepted.** • Taking the risk in order to pursue an opportunity or achieve a benefit/return. • Maintaining exposure to the risk by informed decision.

Stage 4 – Risk reporting & escalation

Reporting

Timely capture, tracking and sharing of risk information is required to enable review and notification to management of changes in the risk environment. It supports understanding and decisions on risk responses to be made, including potential interventions to avoid a risk occurring or reduce its impact.

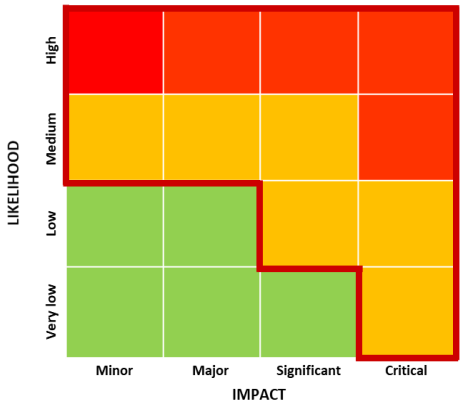
- Each Strategic Director's risk register is to be reviewed, updated and reported to the Risk Management Team on a quarterly basis.
- On a quarterly basis the most significant risks identified in the Strategic Director risk registers will be reported to the Corporate Assurance Group.
- On behalf of the Senior Leadership Team, the Risk Management Team will review and update the Corporate risk register biannually and report this to the Cabinet.

See Appendix 1 – Risk reporting template

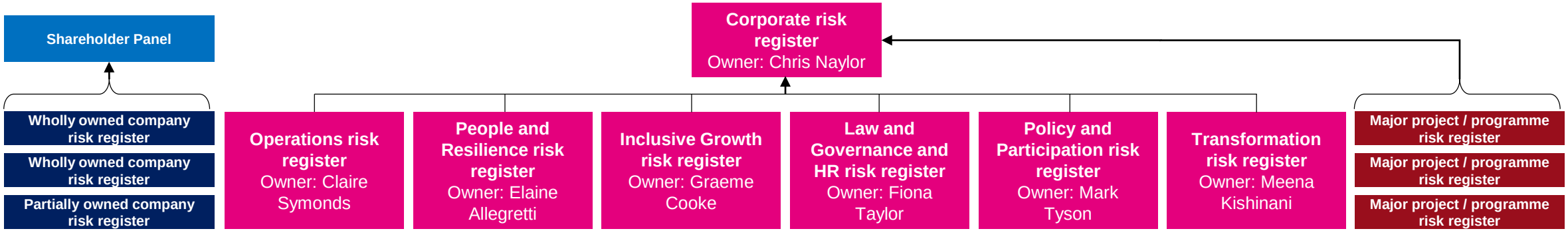
Escalation

The escalation of risks should be timely and accurate. After risks are assessed they should be escalated in line with the following criteria:

- All Red and Amber rated risks identified in the Strategic Director risk registers are to be escalated to the Risk Management Team as part of the quarterly reporting process.
- The Risk Management Team will escalate to the Corporate Assurance Group if necessary in the next quarterly report.



Stage 4 – Risk reporting & escalation - Risk register ownership



Corporate risk register

The most significant risks identified in LBBD will be recorded in the corporate risk register. The corporate risk register is reviewed and challenged biannually.

Chief Officer risk registers

Each Chief Officer is responsible for monitoring and escalation of their identified risks and providing quarterly risk updates to the Risk Management Team.

Major project / programme risk registers

A risk register should also be in place for each of LBBD's major projects and/or programmes.

Wholly and partially owned companies' risk registers

In addition, wholly and partially owned companies must own and manage a separate risk register and are required to share this with the Shareholder Panel on a quarterly basis. Risks that are shared between LBBD and a company should be recorded on both risks registers. A risk owner should be identified from both LBBD and the company and it should be clear who is responsible for each element of the risk.

Further information and contacts

Further information and contacts

For further information about any aspect of the risk management approach:

Christopher Martin, Head of Assurance

Telephone : 020 8227 2174 | 07870 278188
Email : Christopher.Martin@lbbd.gov.uk

Appendix 1 – Risk reporting template

1. Risk title

Risk Owner	[Insert Owner]
Risk Description	[Insert risk description]

	Inherent Risk	Net Risk	Target Risk
Impact			
Likelihood			

Controls	Further Action(s)	Action Owner	Delivery Due Date
[Insert Control]	[Insert further action]	[Insert action owner]	[Insert due date]

Additional comments on this risk	**[Insert further comments]**

This page is intentionally left blank

AUDIT AND STANDARDS COMMITTEE

3 February 2020

Title: Work Programme 2019/20 and Terms of Reference Comparison	
Report of the Director of Law and Governance	
Open Report	**For Information**
Wards Affected: None	**Key Decision:** No
Report Author: Masuma Ahmed, Democratic Services Officer	**Contact Details:** E-mail: masuma.ahmed@lbbd.gov.uk
Accountable Strategic Leadership Director: Fiona Taylor, Director of Law and Governance	

Summary:

The Audit and Standards Committee has a broad range of responsibilities as shown in its terms of refence, specifically Internal and External Audit, Governance, Finance and Standards. Following a review of its work and a potential overlap with the Overview and Scrutiny Committee after its inception in May 2018, amended terms of reference for the Committee were agreed at Assembly in May 2019.

At its meeting on 23 July 2019, the Committee received the regular report on its work programme for 2019/20 and asked officers to include details in the report to this meeting showing how the Committee fulfils its terms of reference against the annual work programme.

Attached at Appendix A is the extract from the Council Constitution showing the Committee's terms of reference. Details of the reports submitted during the past 12 months and/or those scheduled to be presented under the current work programme are shown in ***bold italics*** within that document.

There are several aspects within the terms of reference that have not been considered by the Committee during the past year and are not scheduled to be over the coming months. This is perfectly normal as the terms of reference are intended to cover all areas of potential responsibility for the Committee. For example, reports to the Committee relating to customer complaints and Local Government Ombudsman (LGO) enquiries (paragraph 2.1.1(x)) would typically stem from issues or concerns expressed as part of an internal audit into the Council's processes or from the recommendations of an LGO investigation. Similarly, the Committee would only be expected to review the audit aspects of the Council's Financial Regulations and Rules (paragraph 2.1.1(xii)) as part of a wider review of those Rules.

The Committee's work programme for the remainder of the 2019/20 municipal year is set

out at Appendix B.

The Chief Operating Officer will provide an update on the reports that were due to be presented at this meeting but were held back due to circumstances arising. For this reason, the previous version of the Work Programme has been provided at Appendix B.

Recommendation(s)

The Committee is asked to:

(i) Note the terms of reference and the comparison, as set out at Appendix A to the report; and

(ii) Note the verbal update from the Chief Operating Officer as to the reports that were on the Work Programme but could not be presented at today's meeting; and

(iii) Note the other items on the Work Programme.

Public Background Papers: None

List of appendices:

Appendix A	Terms of Reference for the Audit and Standards Committee (including detail of reports in the work programme for 2019/20)
Appendix B	Work Programme 2019/20

Extract from the Constitution, Part 2, Chapter 13

Audit and Standards Committee

2. Responsibility for Functions:

2.1 The Audit and Standards Committee shall have the following roles and functions:

2.1.1 **Audit functions**

Internal Audit

i) Considering regular update reports concerning the work of Internal Audit, including progress on delivering the annual programme of work, emerging themes, risks and issues, and officer responsiveness in implementing recommendations and responding to Internal Audit.

- ***16/01/19: Internal Audit 2018/19 Quarter 2 and Counter Fraud 2018/19 Quarter 2***
- ***03/04/19: Internal Audit 2018/19 Quarter 3 and Counter Fraud 2018/19 Quarter 3***
- ***28/10/19: Internal Audit 2019/20 Quarters 1 &2 and Counter Fraud 2019/20 Quarters 1 &2***
- ***03/02/20: Internal Audit 2019/20 Quarter 3 and Counter Fraud 2019/20 Quarter 3***

ii) Considering and agreeing an Annual Audit Report from the Chief Financial Officer and a summary of Internal Audit activity (actual and proposed), and the level of assurance it can give over the Council's corporate governance, internal control, and risk management arrangements.

- ***23/07/19: Internal Audit Annual report 2018/19***
- ***23/07/19: Counter Fraud Annual report 2018/19***
- ***03/04/19: Draft Internal Audit Charter, Strategy and Plan 2019/20***
- ***27/04/20: Internal Audit Charter, Strategy and Plan 2020/21***

iii) Considering summaries of specific Internal Audit reports as requested.

iv) Considering reports dealing with the management and performance of the providers of Internal Audit services.

Statutory and External Audit Functions

v) Considering the Annual Governance Report (both main and pension) and other relevant reports.

- ***03/02/20: Annual Governance Statement: update on progress***

vi) Considering the Annual Audit Letter, and other relevant reports.

- ***16/01/19: Annual Audit Letter 2017/18***
- ***16/01/19: External Audit Plan 2018/19***
- ***03/04/19: External Audit Plan Interim Report***
- ***23/07/19: External Audit report 2018/19***
- ***28/10/19: Progress Update on External Audit of 2018/19 Accounts***
- ***28/10/19: External Audit 2018/19 Progress update***
- ***03/02/20: Preparation of the External Audit 2019/20***
- ***03/02/20: External Audit Plan 2020/21***

vii) Considering the Summary of Grant Certifications**.**

- ***Report on 03/04/20***
- ***Report on 03/02/20***

viii) Considering other specific reports as agreed with the external auditor.

Governance

ix) Receiving reports and making appropriate recommendations concerning corporate governance, risk management, decision-making and information governance and ensuring compliance with best practice.

- ***16/01/19: Information Governance Annual Report***
- ***28/10/19: Risk Management Framework Update***
- ***03/02/20: Information Governance Annual Report***
- ***27/04/20: Risk Management Framework – end of year report***

x) Receiving reports and making appropriate recommendations concerning customer complaints and Local Government Ombudsman enquiries.

xi) Considering regular updates concerning Council policies relating to internal governance (including whistleblowing, bribery and anti-fraud) and ensuring the implementation of relevant legislation relating to governance, fraud and corruption.

- ***28/10/19: Review of Key Counter Fraud Policies and Strategy)***

xii) Considering proposed changes to the Council's Financial Regulations and Rules, as they relate to audit functions.

xiii) Approving the Council's Annual Governance Statement which accompanies the Annual Statement of Accounts.

- ***23/07/19: Annual Governance Statement 2018/19***

Finance

xiv) Considering and approving the Annual Statement of Accounts and all related documents.

- ***16/01/19: Preparation of 2018/19 Annual Accounts and External Audit***
- ***23/07/19: Approval of the Statement of Accounts 2018/19***
- ***23/07/19: External Audit report 2018/19***
- ***28/10/19: Progress Update on External Audit of 2018/19 Accounts***
- ***28/10/19: External Audit 2018/19 Progress update***
- ***03/02/20: Preparation of the External Audit 2019/20***

2.1.2 **Standards functions**

i) Promoting and maintaining high standards of conduct by Members and Co-Opted Members of the authority;

ii) Appointment of a Hearing Sub-Committee to hear and make recommendations to the Monitoring Officer concerning complaints about Members and Co-opted Members referred to it by the Monitoring Officer (the composition, Terms of Reference and responsibility of functions for the Sub-Committee are referred to in paragraphs 3 and 4 below);

iii) Receiving periodic reports from the Monitoring Officer on dispensations granted / refused, complaints received against Members, complaints resolved informally, complaints resolved after an investigation by the Hearing Sub-Committee and assessing the operation and effectiveness of the Members' Code of Conduct**;**

- ***16/01/19: Complaints against Members update***
- ***16/01/19: Review of Gifts and Hospitality***
- ***23/07/19: Complaints against Members update***
- ***03/02/20: Standards Complaints update (including Gifts and Hospitality)***

iv) Advising on training or arranging to train Councillors and Co-opted Members on matters relating to the Councillors' Code of Conduct;

v) Assisting Councillors and Co-opted Members to observe the Councillors' Code of Conduct;

vi) Receiving referrals from the Monitoring Officer into allegations of misconduct, in accordance with the Council's assessment criteria;

vii) Advising on the contents of and requirements for codes / protocols / other procedures relating to standards of conduct throughout the Council;

viii) Maintaining oversight of the Council's arrangements for dealing with complaints;

ix) Informing the Assembly and the Chief Executive of relevant issues arising from the determination of Code of Conduct complaints;

x) On referral by the Monitoring Officer, granting dispensations pursuant to S33(2) (b), (c) and (e) of the Localism Act 2011 to enable a Councillor or Co-opted Member to participate in a meeting of the Authority;

xi) Hear and determine appeals against refusal to grant dispensations by the Monitoring Officer pursuant to S33(2)(a) and (d) of the Localism Act 2011.

Appendix B

Audit and Standards Committee - Work Programme 2019/20 Chair: Councillor Princess Bright				
Meeting	**Agenda Item**	**Lead Officer**	**Final Papers deadline**	**Publication Date**
3 February 2020 19:00 Town Hall, Barking	1. ISA 260 and Annual Audit Letter 2. Internal Audit report Quarter 3 19/20 3. Counter Fraud report Quarter 3 19/20 and Review of Key Counter Fraud Policies and Strategy 4. Risk Management Framework Update and 6 monthly report 5. Preparation of the External Audit 2019/20 and Approval of Statement of Accounting Policies 2019/20 - *to be rescheduled* 6. Certificate of Grants and Claims – *to be rescheduled* 7. Work Programme 2019/20 and Terms of Reference Comparison	Tom Mulloy / BDO Chris Martin Chris Martin / Kevin Key Chris Martin Tom Mulloy BDO Democratic Services	**21 January 2020**	**24 January 2020**

27 April 2020 19:00 Town Hall, Barking	1. External Audit Plan 2019/20 2. Internal Audit Charter, Strategy & Plan 2020/21 3. Risk Management Framework (end of Year report) 4. Information Governance Annual report 5. Annual Governance Statement Review 6. Standards Update - Complaints and Gifts & Hospitality 7. Work Programme 2020/21	BDO Chris Martin Chris Martin Claire Symonds Chris Martin Fiona Taylor / Paul Feild Democratic Services	**14 April 2020**	**17 April 2020**

First meeting of the 2020-21 Municipal Year

- **Provisional** date: 27 July 2020 – agenda items to be scheduled.

  (Other 2020-21 meetings dates to be confirmed)