West Midlands Fire and Rescue Authority

Audit Committee

You are summoned to attend the meeting of Audit Committee to be held on Monday, 06 June 2016 at 12:30

at Fire Service HQ, 99 Vauxhall Road, Nechells, Birmingham B7 4HW

for the purpose of transacting the following business:

Agenda – Public Session

13 Committee Members' Private Meeting with External Auditors

Distribution:

Adam Aston - Member, Tersaim Singh - Chairman, Hendrina Quinnen - Member, Robert Sealey - Member, Paul Singh - Member, Catherine Miks - Member

Agenda prepared by Julie Connor

Strategic Hub, West Midlands Fire Service

Tel: 0121 380 6906 email: strategichub@wmfs.net

This agenda and supporting documents are also available electronically on the West Midlands Fire Service website at www.wmfs.net

Minutes of the Audit Committee

11 April 2016 at 12.30 pm
at Fire Service Headquarters, Vauxhall Road, Birmingham B7 4HW

Present: **Councillors T Singh, Aston, Miks, Quinnen, Sealey and Barrie**
Mr Ager (Independent Member)

Apology: **Cllr P Singh**

9/16 **Minutes of the Audit Committee held on 18 January 2016**

Resolved that the minutes of the meeting held on 18 January 2016, be approved as a correct record.

10/16 **Audit Committee Terms of Reference**

The Committee considered the existing Audit Committee Terms of Reference in line with the guidance from CIPFA. Following the review, it was felt that the Terms of Reference were fit for purpose and no changes had been made in the previous twelve months.

Resolved that following a review of the terms of reference that the existing terms of reference be approved.

11/16 **Internal Audit Plan 2016/17**

The Committee received the internal audit plan for the period 2016/17, together with an indicative plan covering the period 2017/18 to 2018/19. The plan would remain fluid and be kept under review and any proposed changes would be reported to the Committee for approval.

The Internal Auditor outlined the audit planning process and steps taken. The Audit Universe (a list of areas that may require auditing) is identified by a variety of methods; the strategic risk register, mandatory areas, such as the key financial systems and areas where the auditor's knowledge, managers requests and past experience are used.

The CIPFA scoring methodology is used to score auditable areas as high, medium or low risk and then identify the areas where assurance will be provided in 2016/17.

- High risk areas will be audited annually,
- Medium risk may be visited once in a three year cycle
- A watching brief remains on low risk areas

Resolved that the internal audit plan for 2016/17 be approved.

12/16 **Audit Plan 2015/16**

Approval was sought to Grant Thornton's Audit Plan 2015/16 which set out the audit work Grant Thornton would undertake in respect of the Authority's financial statements and the delivery of its value for money conclusion on the Authority's arrangements to secure economy, efficiency and effectiveness.

The code of Audit Practice requires Grant Thornton to issue a value for money conclusion. The conclusion will be based upon the same two reporting criteria used in the 2014/15 audit, namely that the Authority has proper arrangements in place for:

- Securing financial resilience
- Challenging how it secures economy, efficiency and effectiveness in its use of resources

The Auditors have determined the overall Materiality level to be £2,368k (being 2% of gross revenue expenditure).

If any errors are identified they would be reported to Audit Committee. The Auditor would give close scrutiny to cash and cash equivalents, disclosures of officers' remuneration, salary bandings and exit packages in notes to the statements and related party transactions.

1) The Audit Plan set out the key phases and activities for the delivery of the audit work. The statutory deadline for submitting the 2015/16 accounts for approval by the Authority is 30 September 2016, when the auditor is required to issue the opinion and value for money conclusion. However, it is the intention to bring the process forward with the accounts being approved by the Audit Committee and the Auditor issuing the opinion and value for money conclusion by 31 July 2016. The audited 2015/16 accounts will be submitted to the Audit Committee for approved by 30 September 2016 when the Auditor aims to issue the opinion and value for money conclusion.

2) An initial risk assessment has already been carried out and no significant risks had been identified. The Auditor proposed to address the risks associated with the Local Government Financial Settlement 2016/17, working with partners, other third parties and the Home Office during the audit of accounts.

The Interim Audit Work had not identified any areas of weakness. The fees and independence were also confirmed.

The Vice Chair thanked the Auditor for making the report clear and easy to understand.

In response to a Member's question on the Auditors reliance on internal audit of Payroll and Pension, the External Auditor confirmed that audit testing always started with Internal Audit, but they would test further if a problem was highlighted.

The Deputy Chief Fire Officer responded to a Member's enquiry about Partnership working and confirmed that the Authority faced an uncertain phase in respect of governance arrangements because of the Combined Authority and Police and Crime Bill. The Authority have secured Observer status on the Combined Authority and were continuing to move forward with Community based working.

Resolved that the Grant Thornton's Audit Plan to enable the delivery of the audit of financial statements and the value for money conclusion 2015/16 be approved.

13/16 **Corporate Risk Quarter 3 Update 2015/16**

The Committee received the Corporate Risk Assurance Map and noted the position statement detailing the work undertaken in support of the management of each of the Service's Corporate Risks.

Corporate Risks were those which, if they occurred, would seriously affect the Authority's ability to carry out its core functions or deliver its strategic objectives as set out in The Plan. The Authority currently had eleven corporate risks. The Corporate Risk Assurance Map summary provided a description of each risk and an overview of its rating. The position statement set out the outcomes of the regular review of each risk by the risk owner. The Committee noted the position with regard to each risk and the confidence ratings. The Committee noted that there were 7 green and 4 amber overall confidence ratings.

The Committee noted that Corporate Risks 5, 6, 11 and 13 had been realigned to reflect the recent changes to the Strategic Enabling Team.

Corporate Risks 1 and 5 were still indicated as high risk due to the ongoing trade dispute and pensions dispute (this was dormant at the moment but may comeback).

A member enquired about the risk of working with partners and where it should be reported.

The Deputy Chief Fire Officer agreed this was obviously missing in the risk reporting and Officers were looking at partnerships and felt that this area of work may need its own risk. Officers were looking at all Corporate Risks and it was felt a fundamental change would be required to take account of all the possible changes in the future, including the Combined Authority.

Resolved that the Corporate Risk Assurance Map summary be approved.

14/16 **Frequency of Corporate Risk Reporting to Audit Committee**

The Committee received a report requesting a change in frequency for the provision of the overall corporate risk position statement updated from four times a year to twice a year. It was felt that changes are needed to the risk assurance map and the introduction of regular reports to the Committee would provide timely and specific corporate risk information.

It was proposed to reduce the frequency of corporate risk position statements reporting from four times a year to every six months. Risk reporting will be by exception with a full report every six months. Interim meetings would be used to report changes to risks and enable focused discussions on specific risks as and when they emerge in the organisation and this approach will promote and enable Members to become more aware of specific, risk critical issues in a timely way.

The Deputy Chief Fire Officer had discussed the proposed approach with both the Treasurer and Internal Auditor.

Members considered a sample of an Audit Committee briefing, however, one Member felt that it was a primary task of the Audit Committee to consider risk and would be unhappy if risks didn't appear at Audit Committee and asked that when bringing reports on particular

risks that the Risk Owner attend the Audit Committee to provide further details. The Deputy Chief Fire Officer agreed to this suggestion.

Resolved:

(a) that the change of frequency for providing the Committee with an overall corporate risk position statement update from four times a year to twice a year be approved.

(b) That the introduction of regular reports to Committee to provide timely and specific corporate risk information as a means of keeping members fully engaged in and aware of the emerging corporate risk matters be approved.

15/16 **External Audit Work Programme and Scale of Fees**

The Committee noted the external audit work programme and scale of fees for the 2016/17 audit work to be undertaken by Grant Thornton UK LLP.

Grant Thornton UK LLP had been appointed to audit the Authority's accounts for a five year period from 2012/13 until 2016/17. James Cook and Emily Mayne would continue in their roles for 2016/17.

The scale of fees was set at £38,636 which is the same charge as 2015/16.

Resolved that the external audit work programme and the scale of fees for 2016/17 be noted.

16/16 **Communication with the Audit Committee for West Midlands Fire and Rescue Service**

The Committee received an update from the Authority's external auditors, Grant Thornton relating to the progress of the external auditors in delivering their responsibilities, which included matters that related to fraud, law and regulations, going concerns, related parties, and accounting estimates.

In answer to a Member's enquiry, Grant Thornton confirmed they were content with the responses received from the Treasurer and there was a strong dialogue with the Treasurer and Finance Manager.

17/16 **Audit Committee Update for West Midlands Fire and Rescue Authority**

The Committee received and noted an update from its external auditor which set out Grant Thornton's progress in delivering its responsibilities and a summary of emerging national issues and developments which might impact on the Authority and a number of change questions in respect of those emerging issues.

Good progress had been made with the preliminary 2015/16 Audit and the Auditor was on track to complete the final audit accounts early. The deadline had changed to July from September to reflect the early close off of account and completion of the Audit. The Annual Audit letter was planned for October 2016.

The Committee were provided with a number of challenge questions and informed of the challenges facing local government in respect of the financial settlement, a CFO Insights online tool, an invaluable tool providing focused insight to development and the evidence to support financial decisions.

Grant Thornton had published a report on Collaboration in Mental Health. The Fire Service has a dedicated member of staff working with the Mental Health Trust, Police and Ambulance Services and the Auditor agreed to provide a copy at the next meeting of the Audit committee.

18/16 **Internal Audit - Progress Report**.

The Committee noted a report from the internal auditor which detailed the progress made against the delivery of the 2015/16 Internal Audit Plan.

The information contained within the report would inform the overall opinion in the Internal Audit Annual Report at the end of the year. There was a substantial level of assurance to the end of January and there was nothing to suggest that the Authority would not receive a Qualified Opinion.

19/16 **Notes of the Pensions Board held on 8 February 2016**

The Committee received the minutes of the Pensions Board meeting held on 8 February 2015. The Finance Manager had attended the meeting where the Board had received supporting information from the Payroll and Pensions Manager together with the activity levels of the Pensions Section. It was noted that following the Gad v Milne case, approximately £6.75m had been paid out on 1 February to pensioners who were affected by the outcome of this case, but that the payment received from the Department of Communities and Local Government had been late. The next meeting of the Pensions Board was scheduled to take place on 11 July 2016.

20/16 **Audit Committee Work Programme 2015/16**

The Committee noted its Work Programme for 2015/16.

21/16 **Update on Topical, Legal and Regulatory Issues**

There was no new information to be presented

(The meeting ended at 12:56 pm)

Contact Officer: Julie Connor
Strategic Hub
0121 380 6906

WEST MIDLANDS FIRE AND RESCUE AUTHORITY

AUDIT COMMITTEE

6 JUNE 2016

1. GOVERNANCE STATEMENT 2015/2016

Joint report of the Chief Fire Officer, Treasurer and Monitoring Officer.

RECOMMENDED

THAT the Committee considers and comments on the Governance Statement for 2015/2016.

2. PURPOSE OF REPORT

This report is submitted to Members to seek comments and consideration of the Governance Statement for 2015/2016.

3. BACKGROUND

3.1 West Midlands Fire and Rescue Authority is responsible for ensuring that its business is conducted in accordance with the law and proper standards, and that public money is safeguarded and properly accounted for and used economically, efficiently and effectively. The Authority also has a duty under the Local Government Act 1999 to make arrangements to secure continuous improvement in the way in which its functions are exercised, having regard to a combination of economy, efficiency and effectiveness.

3.2 In discharging this overall responsibility, the Authority is also responsible for putting in place proper arrangements for the governance of its affairs, which includes arrangements for the management of risk.

3.3 Every Local Authority has to produce a Governance Statement (see attached Appendix 1) with its Statement of Accounts, which are due to be made available at the end of June 2016.

3.4 The Governance Statement is designed to manage risk to a reasonable level rather than to eliminate all risk of failure to achieve policies, aims and objectives; it can, therefore, only provide reasonable and not absolute assurance of effectiveness. The Governance Statement is based on an ongoing process designed to identify and prioritise the risks to the achievement of the Authority's policies, aims and objectives, to evaluate the likelihood of those risks being realised and the impact should they be realised, and to manage them efficiently, effectively and economically.

3.5 The Statement is signed by the Chairman of the Authority and the Chief Fire Officer who have a responsibility to ensure that the document is supported by reliable evidence and accurately reflects the Authority's internal control environment. The Governance Statement has operated throughout the year ended 31st March 2016 and up to the date of the approval of the annual report and accounts.

4. EQUALITY IMPACT ASSESSMENT

In preparing this report an initial Equality Impact Assessment is not required and has not been carried out because the matters contained in this report do not relate to a policy change.

5. LEGAL IMPLICATIONS

The Authority has a duty under the Local Government Act 1999 to make arrangements to secure continuous improvement in the way in which its functions are exercised, having regard to a combination of economy, efficiency and effectiveness. As part of this it has to produce a Governance Statement.

6. FINANCIAL IMPLICATIONS

There are no direct financial implications arising from this report.

The contact name for this report is Deputy Chief Fire Officer Philip Hales, Telephone No: 0121 380 6907.

PHIL LOACH	MIKE GRIFFITHS	MELANIE DUDLEY
CHIEF FIRE OFFICER	TREASURER	MONITORING OFFICER

Ref. AU/Audit/Jun/21705167/KS/GVH

APPENDIX 1

ANNUAL GOVERNANCE STATEMENT

1. Scope of Responsibility

1.1 West Midlands Fire and Rescue Authority is responsible for ensuring that its business is conducted in accordance with the law and proper standards, that public money is safeguarded and properly accounted for and used economically, efficiently and effectively. The Authority also has a duty under the Local Government Act 1999 to make arrangements to secure continuous improvement in the way in which its functions are exercised, having regard to a combination of economy, efficiency and effectiveness.

1.2 In discharging this duty, the Authority is also responsible for putting in place proper arrangements for the governance of its affairs which facilitates the effective exercise of the Authority's functions and which includes arrangements for the management of risk.

1.3 The Authority has complied with the code of corporate governance which is consistent with the principles of the CIPFA/SOLACE Framework – Delivering Good Governance in Local Government and has also complied with the requirements of CIPFA's statement on the role of the Chief Financial Officer in Local Government. This Annual Governance Statement explains how the Authority has complied with the code and also meets the requirements of Accounts and Audit (England) Regulations 2011, regulation 4 (3) which require the Authority to prepare an Annual Governance Statement.

2. The Purpose of the Governance Framework

2.1 The governance framework comprises the systems and processes, culture and values by which the Authority is directed and controlled and its activities through which it accounts to and engages with the community. It enables the Authority to monitor the achievement of its strategic objectives and to consider whether those objectives have led to the delivery of appropriate, value for money services.

2.2 The system of internal control is a significant part of the framework and is designed to manage risk to a reasonable level. It cannot eliminate all risk of failure to achieve policies, aims and objectives and can, therefore, only provide reasonable and not absolute assurance of effectiveness. The system of internal control is based on an ongoing process designed to identify and prioritise the risks to the achievement of the Authority's policies, aims and objectives, to evaluate the likelihood and potential impact of those risks being realised and the impact should they be realised and to manage them efficiently, effectively and economically.

2.3 The governance framework has been in place for the year ended 31st March 2016 and up to the date of the approval of the annual report and statement of accounts.

3. The Governance Framework

The key elements of the systems and processes that comprise the Authority's governance arrangements include the following:-

3.1 The Authority has produced a Corporate Strategy setting out its objectives and there is regular performance monitoring in which achievement of the Authority's objectives is measured and monitored.

3.2 The Authority has established clear channels of communication with the community and stakeholders regarding the production of the Annual Report and consultation on the key priorities of the Service. This also encourages open communication.

3.3 The Authority facilitates policy and decision-making via regular Policy Planning Forums and Authority and Executive Committee meetings. An Audit Committee provides independent assurance to the Authority on risk management and internal control and the effectiveness of the arrangements the Authority has for these matters. The constitution of the Committees including the terms of reference is reviewed annually and available on the Internet.

3.4 The Authority ensures compliance with established strategies, procedures, laws and regulations – including risk management. The Authority also maintains and reviews regularly its code of conduct and whistle blowing policy. There is a comprehensive induction programme in place and information regarding strategies and procedures are held on the intranet, which continues to be developed. The Authority has a strong Internal Audit function and established protocols for working with External Audit.

3.5 West Midlands Fire and Rescue Authority will continue to enhance and strengthen its internal control environment through the review of current policies and procedures.

3.6 The Authority has corporate risk management arrangements in place which are supported by an approved Risk Management Strategy enabling Managers and other senior officers to identify, assess and prioritise risks within their own work areas which impact on the ability of the Authority and its services to meet objectives. To consider the effectiveness of the Authority's risk management arrangements is a specific term of reference for the Audit Committee and risk management is a specific responsibility of both the Chairman and Vice Chairman.

3.7 The Authority's Corporate Risk Register identifies the principal risks to the achievement of the Authority's objectives and assesses the nature and extent of those risks (through assessment of likelihood and impact). The Register identifies risk owners whose responsibility includes the identification of controls and actions to manage them efficiently, effectively and economically.

3.8 The Authority ensures the economical, effective and efficient use of resources, and secures continuous improvement in the way in which its functions are exercised, by having regard to a combination of economy, efficiency and effectiveness as required by the Best Value duty. The Authority plans its spending on an established planning cycle for policy development, budget setting and performance management through the business planning process. This ensures that resources are aligned to priorities and secures best value from the resources that are available.

3.9 The Chief Financial Officer is a key member of the leadership team, helping to develop and implement the Authority's strategy. The Authority's financial system is an ORACLE based general ledger and management information system, which integrates the general ledger function with those of budgetary control and payments. Financial Regulations and Contract Procedure Rules are approved and regularly reviewed by the Authority. A rigorous system of monthly financial monitoring ensures that any significant budget variances are identified in a timely way, and corrective action initiated.

3.10 The Authority's performance management and reporting of performance management continues to be improved with a more focused Corporate Strategy, the setting of priorities and is supported by regular performance monitoring. Corporate performance is reported on a quarterly basis and this process provides officers and Members with the opportunity to share knowledge and understanding about key performance issues affecting services.

3.11 The Authority has a Standards Committee which promotes high ethical standards amongst Members and has one independent member. This Committee leads on developing policies and procedures to accompany the revised Code of Conduct for Members and is responsible for local assessment and review of complaints about members' conduct. The Authority also has a Scrutiny Committee which undertakes performance management functions and informs policy development.

3.12 The Fire and Rescue National Framework for England sets out a requirement for Fire and Rescue Authorities to publish 'Statements of Assurance'. Specifically, Fire and Rescue Authorities must provide assurance on financial, governance and operational matters and show how they have had due regard to the expectations set out in their integrated risk management plan and the requirements included in this Framework. The Authority has approved the Statement of Assurance which is available on the Service's website.

4. Review of Effectiveness

4.1 The Authority has responsibility for conducting, at least annually, a review of the effectiveness of its governance framework including the system of internal control. The review of effectiveness is informed by the work of the statutory officers and principal managers of the Authority who have responsibility for the development and maintenance of the governance environment, the internal audit annual report and comments made by the external auditors in their annual audit letter and other reports.

4.2 Department and section unit business plans contain a variety of performance indicators and targets that are regularly reviewed.

4.3 The Authority's political governance arrangements, which are appropriately reviewed by officers, set out the responsibilities of both Members and senior managers. In particular the Authority has identified the following statutory post holders:-

- Chief Fire Officer
- Treasurer
- Monitoring Officer

In addition to the statutory posts, the post of Clerk to the Authority has been maintained.

4.4 The arrangements for the provision of internal audit are contained within the Authority's Financial Regulations. The Treasurer is responsible for ensuring that there is an adequate and effective system of internal audit of the Authority's accounting and other systems of internal control as required by the Accounts and Audit Regulations 2003 as amended in 2006. The internal audit provision operates in accordance with the CIPFA Code of Practice for Internal Audit in Local Government 2006. The Authority's Audit Plan is prioritised by a combination of the key internal controls, assessment and review on the basis of risk and the Authority's corporate governance arrangements, including risk management. The work is further supplemented by reviews around the main financial systems, scheduled visits to Authority establishments and fraud investigations. Internal Audit leads on promoting a counter-fraud culture within the Authority.

4.5 The resulting Audit Plan is discussed and agreed with officers of the Strategic Enabling Team and the Audit Committee and shared with the Authority's external auditor. Meetings between the internal and external auditor ensure that duplication of effort is avoided. All Authority Audit reports include an assessment of the adequacy of internal control and prioritised action plans to address any areas needing improvement.

4.6 The Authority's review of the effectiveness of the system of internal control is informed by:-

- The work undertaken by Internal Audit during the year;
- The work undertaken by the external auditor reported in their annual audit;
- Other work undertaken by independent inspection bodies.

4.7 From the work undertaken by Internal Audit in 2015/2016 the Internal Audit has given a 'reasonable assurance' that the Authority has adequate and effective governance, risk management and internal control processes. This represents an unqualified opinion and the highest level of assurance available to Audit Services. In giving this opinion it is recognised that assurance can never be absolute. The most that internal audit can provide is reasonable assurance that there are no major weaknesses in the Authority's governance, risk management and control processes.

4.8 The Authority is able to confirm that its financial management arrangements conform to the governance requirements of the CIPFA Statement on the Role of the Chief Financial Officer in Local Government (2010).

4.9 We have been advised on the implications of the result of the review of effectiveness of the governance framework by the sources noted above and that the arrangements continue to be regarded as fit for purpose in accordance with the Authority's governance framework. The areas to be specifically addressed are outlined in 5.5.

5. Significant governance arrangements within the Authority

5.1 West Midlands Fire & Rescue Authority has a legal duty to provide an efficient, safe and effective fire and rescue service. The key priorities are:-

- Prevention – Safer and healthier communities
- Protection – stronger business communities
- Response – dealing effectively with emergencies

5.2 These form the basis of the Authority's Corporate Strategy known as The Plan 2016-2019 which sets out the outcomes and priorities based on the Community Safety Strategy. The five-minute attendance standard lies at the heart of the Service Delivery Model. The model shows how staff provide the core prevention, protection and response services to make the West Midlands safer, stronger and healthier.

5.3 Grant Thornton, the Authority's External Auditors, published the Audit Findings Report for its 2014/2015 audit work which reported an unqualified opinion on the financial statements. It also issued an unqualified value for money conclusion stating that the Authority had adequate arrangements to secure economy, efficiency and effectiveness in the use of resources.

5.4 Based on audit work undertaken during the year an Annual Internal Audit Report was presented to the Audit Committee on 6 June 2016, Audit work which was completed in 2015/2016 included:-

- Pensions Certification
- Budgetary Control
- Procurement
- Accounts Receivable
- Fixed Asset Accounting/Asset Planning
- Accounts Payable
- Risk Management
- Governance
- Performance Management
- Workforce Planning
- Business Continuity
- IT
- Payroll

5.5 As a result of these audits the following issues were identified:-

- Governance – Members of the Audit Committee will be required to revisit their self assessment of 'good practice and effectiveness' exercise early in the new year.

- Business Continuity – the need to evidence the completion of the annual business assessment for each business continuity plan and to record when incident training has been undertaken.

5.6 All issues highlighted in the Annual Internal Audit Report have been raised with relevant managers and actions have been taken to achieve improvements.

5.7 In February 2016, the Minister for Local Government confirmed the Authority's funding settlement for 2016/17. The core funding reduction of £3.3m in 2016/2017 has been managed by reviews to services and an increase in Council Tax. In addition to the settlement for 2016/17, an offer was made for a multi-year funding settlement. Any Authority wishing to take up the four year funding settlement to 2019/20 would be required to set out their proposals in an efficiency plan. At this stage the offer of a provisional four year settlement by DCLG is considered to be a reasonable basis to formulate medium term financial planning.

5.8 With the trend of cuts to government funding continuing into future years, the Authority faces considerable financial pressures which could result in difficulties to deliver an efficient and effective service, which in turn would increase the risk to the communities of the West Midlands. A key aim for the Authority is to therefore deliver a more efficient and effective service to the community whilst ensuring the stability of the Authority's financial position remains.

6. Certification

6.1 To the best of our knowledge, the governance arrangements, as outlined above have been effectively operating during the year with the exception of those areas identified as requiring improvement. We propose over the coming year to take steps to address the above matters to further enhance our governance arrangements. We are satisfied that these steps will address the need for improvements that were identified during the review of effectiveness and will monitor their implementation and operation as part of our annual review.

_____ _____

John Edwards
Chairman

Phil Loach
Chief Fire Officer

WEST MIDLANDS FIRE AND RESCUE AUTHORITY

AUDIT COMMITTEE

6 JUNE 2016

1. MONITORING POLICIES ON RAISING CONCERNS AT WORK – WHISTLE BLOWING STANDING ORDER 2/20 AND REGULATION OF INVESTIGATORY POWERS ACT 2000

Joint report of the Chief Fire Officer and the Monitoring Officer.

RECOMMENDED

1.1 THAT the Audit Committee notes that there has been One allegation of whistle blowing reported through the Whistle Blowing Policy (SO 2/20) and this matter reached a satisfactory conclusion to all parties involved. There have not been any requests to enact the Regulation of Investigatory Powers Act 2000 in West Midlands Fire Service in the last year up to 31 March 2016.

1.2 THAT the Audit Committee notes the content of the Whistle Blowing Standing Order 2/20 (attached as Appendix 1) and the Data Protection Policy 1998 Standing Order 2/16 (attached as Appendix 2).

2. PURPOSE OF REPORT

This report is submitted to inform the Committee of the monitoring of the referrals under the Whistle Blowing Standing Order and the use of the Regulation of Investigatory Powers Act under the Data Protection Standing Order. Revision of the Data Protection Framework 2/16 are currently being consulted in line with the Employment Relations Framework.

3. BACKGROUND

Whistle Blowing

3.1 The Whistle Blowing Standing Order was consulted on 4th June 2014 and then published 27th November 2014. Minor amendments were made to include names of new personnel who have responsibilities under Whistle Blowing.

This Standing Order will be reviewed and amended every three years or reviewed earlier if required under any changes in legislation.

3.2 In relation to Whistle Blowing; in May 1996 the Committee on Standards in Public Life stated that “All organisations face the risk of things going wrong or of unknowingly harbouring malpractice. Encouraging a culture of openness within an organisation will help: prevention is better than cure.”

3.3 The Public Interest Disclosure Act 1998 sets out a framework for public interest whistle blowing which protects workers from reprisal because they have raised concern about malpractice. Only a disclosure that relates to one of the broad categories of malpractice can qualify for protection under the Act. These include concerns about actual or apprehended breaches of civil, criminal, regulatory or administrative law; miscarriages of justice; dangers to health, safety and the environment and the cover up of any such malpractice. Case law continues to develop this area of law.

3.4 In addition to employees, the Act covers for example, workers, contractors, trainees, agency staff. This list is not exhaustive.

3.5 To be protected, the person blowing the whistle must believe that their disclosure is “in the public interest”, i.e. disclosure is made in the reasonable belief that there is an issue such as wrongdoing in public office or something that presents a risk to the public that warrants disclosure.

3.6 The Committee should note that there has been One allegation of Whistleblowing raised by an employee over the last twelve months using the Whistle Blowing Policy up to 31 March 2016.

Data Protection

3.7 The Data Protection Act 1998 was consulted on and amended to include a policy on surveillance in May 2012. This policy is currently under review and in consultation. The new Data Protection Framework 2/16 is an amalgamation of Standing Order 2/16 Data Protection Act 1998 and Standing Order 2/21 Personal Information.

Regulation of Investigatory Powers

3.8 The Regulation of Investigatory Powers Act 2000 (RIPA) provides a framework for control and supervision of investigatory powers exercised by public bodies, including local authorities, in order to balance the need to protect privacy of individuals with the need to protect others, particularly in light of the Human Rights Act 1998.

3.9 In 2014 West Midlands Fire Service was inspected under RIPA by Office of Surveillance Commissioners (OSC) a report was submitted with clear recommendations, which the Service has delivered. Training was put in place for senior managers to familiarise themselves with RIPA rules and guidelines.

3.10 The Committee should note that the Service has not approved any surveillance under RIPA legislation in the last twelve months up to 31 March 2016.

3.11 The West Midlands Fire Service will continue to raise awareness through training on the Whistle Blowing Policy, Data Protection Policy and RIPA to all of our partners.

4. EQUALITY IMPACT ASSESSMENT

In preparing this report an Equality Impact Assessment is not required, due to the fact that all our policies have Equality Impact Assessments carried out when updating and amending.

5. LEGAL IMPLICATIONS

5.1 Data Protection: Depending on the level and or seriousness of a breach of the Data Protection Act 1998; there are various levels of prosecution ranging from enforcement notices, financial penalties and in extreme cases custodial sentences.

5.2 RIPA: if surveillance operations are not carried out in accordance with the safeguards as laid down in RIPA, the evidence obtained may not be admissible in legal proceedings and the Service may be subject of a claim on infringing the human rights of the person under surveillance.

6. FINANCIAL IMPLICATIONS

Monetary Penalty notices: fines of up to £500,000 for serious breaches of the DPA.

7. ENVIRONMENTAL IMPLICATIONS

There are no environmental implications arising from this report.

BACKGROUND PAPERS

The Public Interest Disclosure Act 1998 (PIDA)

The contact name for this report is Phil Hales, Deputy Chief Fire Officer, telephone number 0121 380 6907.

PHIL LOACH
CHIEF FIRE OFFICER

M DUDLEY
MONITORING OFFICER TO THE AUTHORITY

WEST MIDLANDS FIRE SERVICE

WHISTLE BLOWING POLICY

STANDING ORDER 2/20

October 2015

Employee Relations

People Support Services

WEST MIDLANDS FIRE SERVICE
WHISTLE BLOWING POLICY

1. WHISTLE BLOWING CONTENTS

2. STRATEGY

Following the Public Interest Disclosure Act 1998 (PIDA), which came into force in July 1999, legal protection is now provided to employees who raise concerns about suspected dangerous or illegal activity that they are aware of through their work. The common term for voicing such concerns is 'whistle blowing'. West Midlands Fire Service (WMFS) wishes to create an open and honest culture by being compliant with its statutory obligations, detailed in the Act, and ethical standards, detailed in its Core Values. Details on our core values can be found in the Equality & Diversity Standing Order 0213 or 'The Plan': http://wm-srv-alf-01:8080/share/proxy/alfresco/api/node/content/workspace/SpacesStore/4806b62c-f0c9-4600-a25d-8557d1360ead/The%20Plan%202014-2017.pdf

Employees are often the first to realise that there may be something seriously wrong with the organisation that employs them. They may be able to alert the organisation early on to things like fraud, negligence, bribery and health and safety risks. However, they may not express their concerns, because they feel that speaking up would be disloyal to their colleagues or to the organisation. They may also fear harassment or victimisation. In these circumstances it may be easier to ignore the concern rather than report what may be no more than a suspicion of malpractice.

The procedures in this order give ways for individuals to raise concerns and receive feedback on any action taken. It makes sure that individuals receive a response and know how to pursue concerns if they are not happy with the response. It gives reassurance that individuals will be protected from possible reprisals or victimisation if they believe they have made a disclosure.

3. PROCEDURE

3.1 What the policy covers

The Public Interest Disclosure Act 1998 makes sure that employees, contractors providing services, most agency workers, home workers and trainees on vocational and work experience schemes are legally protected in raising concerns responsibly.

External contractors may encounter wrongdoing that affects WMFS. Therefore, this whistle blowing policy is also open to employees of our contractors.

The subject of concern may be something unlawful, against the Service's policies, below established standards of practice, or that amounts to improper conduct. The overriding concern should be that it would be in the public interest for the alleged malpractice to be corrected.

Whistle blowing is when an employee reports suspected wrongdoing at work. Officially this is called 'making a disclosure in the public interest'.

An employee can report things that aren't right, are illegal or if anyone at work is neglecting their duties, including:

- Someone's health and safety is in danger
- Damage to the environment
- A criminal offence
- The company isn't obeying the law (like not having the right insurance)
- Covering up wrongdoing
- Behaviours that are being displayed

Distinction between grievance and whistle blowing

Whistle blowing occurs when an employee raises a concern about danger or illegality that affects others, not themselves personally. When someone raises a concern

through the Service's grievance procedure, they are saying that they have personally been poorly treated and they are seeking redress or justice for themselves. The whistle blowing policy is intended to cover concerns that fall outside the scope of grievance or other existing Service procedures.

3.2 How to raise a concern

If the matter relates to any fraudulent or corrupt activity, concerns should be raised in accordance with procedures detailed in the Standing Order 1/22, Anti-Fraud, Corruption and Bribery Policy.

If the complainant wishes to raise or discuss any issues which might fall into the above category then the complainant should contact a member of the SET, the Treasurer or the Clerk to the Fire Authority, who will be required by WMFS to treat the matter in confidence.

Where possible, the complainant should raise their complaint in writing setting out the background and history of the concern giving names, dates and places where possible and the reason why the complainant is particularly concerned about the situation. If the complainant does not feel able to put the concern in writing, then the complainant can discuss the concerns verbally with a member of the SET, or the Treasurer or the Clerk to the Fire Authority.

The earlier that the complainant can express the concern and the more detail that can be provided, the easier it will be for the Service to take appropriate and necessary action. Remember:

- the complainant must disclose the information
- the complainant must believe it to be substantially true
- the complainant must not act maliciously or make false allegations
- the complainant must not seek any personal gain

At this stage the complainant will not be expected to prove the allegation, but will need to demonstrate to the person contacted that there are sufficient grounds for reasonable suspicion or concern.

The complainant may invite a member of the trade union representative body or a work colleague to be present during any meetings or interviews in connection with the concerns raised.

Where a concern relates to a Brigade Manager or SET Manager, then either the Strategic Enabler for People (as Responsible Officer), or Deputy Chief Fire Officer or Chief Fire Officer, as appropriate, should be contacted in the first instance. The Assistant Chief Executive, Melanie Dudley at Sandwell MBC has the Monitoring Officer role for the Fire Authority. The Monitoring Officer may be contacted on 0121 569 3513. Address: Sandwell Council House, PO Box 2374, Oldbury, West Midlands, B69 3DE.

The Treasurer to the Fire Authority may be contacted on 0121 3806919. The Clerk to the Fire Authority may contacted on 0121 3806678. Address for the Treasurer and the Clerk to the Fire Authority is: West Midlands Fire Service, 99 Vauxhall Road, Birmingham, B7 4HW.

3.3 Confidentiality

All concerns will be treated in confidence and every effort will be made not to reveal the identity of the complainant. However, it is likely that further investigation will be necessary and the complainant maybe required to attend a disciplinary or investigative hearing as a witness at the appropriate time. An employee raises a concern confidentially if they give their name only on condition that it is not revealed without their consent. A concern is raised anonymously if the employee does not give their name.

3.4 How the Service will respond

The action taken by the Service will depend on the nature of the concern. The matters raised may be investigated internally by an appropriately experienced officer

knowledgeable in the area concerned, for example, audit, Line Manager or HR Practitioner.

Alternatively through the disciplinary process, the matter may be referred to the police, the external auditor or may be the subject of an independent enquiry.

In order to protect individuals and the Service, and those accused of misdeeds or possible malpractice, initial enquiries will be made to decide whether an investigation is appropriate and, if so, what form it should take. Concerns or allegations that fall within the scope of specific procedures, for example, unfair discrimination issues, will normally be referred for consideration under those procedures. Some concerns may be resolved by agreed action without the need for investigation. Members of the SET can seek guidance from the Strategic Enabler of People at any stage in the investigation.

Within 10 working days of a concern being raised, the individual with whom the concern was raised will write to the complainant:

- acknowledging that the concern has been received;
- indicating how the matter is to be dealt with;
- giving an estimate of how long it will take to provide a final response;
- telling the complainant whether any initial enquiries have been made;
- supplying the complainant with information on staff support mechanisms; and
- telling the complainant whether further investigations will take place and if not why not.

The amount of contact between the officer(s) considering the issues will depend on the nature of the matters raised, the potential difficulties involved and the clarity of the information provided. If necessary, further information will be sought from the complainant in a discreet manner.

When any meeting is arranged, the complainant will have the right to be accompanied by a representative body or a work colleague. The meeting can be held off site if requested.

West Midlands Fire Service will take steps to minimise any difficulties, which may be experienced as a result of raising a concern and provide any appropriate support. For instance if required to give evidence in disciplinary or criminal proceedings, the Service will advise the complainant of the procedure and give reasonable support. Subject to legal constraints, complainant will receive information about the outcomes of investigations.

Upon completion of the investigation, **all** documents will be forwarded to the Strategic Enabler of People.

3.5 Responsible officer

The Strategic Enabler of People has overall responsibility for the maintenance and operation of this policy. This officer maintains a record of concerns raised and the outcomes (but in a form which does not endanger the complainant's confidentiality) and will report as necessary to the Service.

3.6 Harassment or victimisation

West Midlands Fire Service recognises that the decision to report a concern can be a difficult one to make, not least because of the fear of reprisal from those responsible for the alleged malpractice. The Service will not tolerate harassment or victimisation and will take action to protect the complainant when a concern is raised.

3.7 Untrue allegations

If the complainant makes an allegation, but it is not confirmed by the investigation, no action will be taken against the complainant. If however the complainant makes an allegation which, upon full investigation, is found to have been malicious or vexatious, disciplinary action will be considered and the protection of the PIDA will be lost.

3.8 Anonymous allegations

This policy encourages the complainant to put their name to the concerns. Concerns expressed anonymously are much less powerful, but will be considered at the discretion of the Strategic Enabler of People.

In exercising this discretion the factors to be taken into account would include the:

- seriousness of the issues raised;
- credibility of the concern; and
- likelihood of confirming the allegation from attributable sources and information provided.

3.9 How the matter can be taken further

This policy is intended to provide the complainant with an avenue to raise concerns within the Service. We hope the complainant will be satisfied with the response. If not, the complainant must indicate this to the Strategic Enabler of People or the Treasurer or Clerk or Monitoring Officer to the Fire Authority.

Legal advice may be sought on any concerns about malpractice. If the employee feels it is right to take the matter outside the Service, the following are possible contacts:

- The complainant's recognised trade union
- Citizens Advice Bureau
- A solicitor
- The Police
- Relevant professional bodies or regulatory organisations, such as Ombudsmen.

Public Concern at Work (www.pcaw.co.uk) is a charity that offers free advice to people concerned about danger or malpractice in the workplace, but who are unsure whether, or how, to raise the matter.

4. CROSS REFERENCES

This Standing Order makes reference to and complements issues contained in other Orders, namely:

Standing Order No. 1/22	Anti-Fraud, Corruption and Bribery Policy
Standing Order No. 2/1	Disciplinary Procedure
Standing Order No. 2/17	Dignity at Work

5. KEY CONSULTEES

Minor changes only have been made to this Order and consultation was not necessary.

6. EQUALITY AND DIVERSITY

The initial Equality Impact Assessment raised no issues so a full impact assessment was not required.

7. OWNERSHIP

This Standing Order did not require Authority or SET approval.

8. RESPONSIBILITY AND REVIEW/AMENDMENT

8.1 Responsible SET Member/Department

Strategic Enabler People/HR Employee Relations Team

8.2 Created/fully reviewed/amended

This Standing Order has been reviewed, amended by Employee Relations in November 2014 and amended in October 2015.

WEST MIDLANDS FIRE SERVICE
DATA PROTECTION ACT 1998

1. STRATEGY

That the West Midlands Fire and Rescue Authority (hereinafter to be known as the Authority) and the West Midlands Fire Service (hereinafter to be known as the Service) fully endorse and adhere to the principles of the Data Protection Act 1998.

The Authority regards the lawful and correct treatment of personal information as very important to successful operations, and to maintain confidence between service users, employees including temporary and volunteers and those communities we serve. The Authority is committed to respecting all rights of those individuals whose personal data it processes and will ensure personal information will be treated lawfully and correctly in accordance with the legislation. It will adopt best practice as designated by the Information Commissioner's Office where possible.

The Information Commissioner's Office is the data protection regulator for the United Kingdom. Its responsibility is to publish guidance on and enforce compliance with the Data Protection Act 1998, Freedom of Information Act 2000, Environmental Information Regulations 2004 and the Electronic Information Regulations 2003.

The Service has defined a number of distinctive roles to manage data protection.

Data Protection Officer	Data Management Officer
Internal Data Controller	Senior member of staff from each function responsible for data management within their respective function. Also to be the liaison point for the Data Protection Officer.
Data User	All those that handle data. All individuals have a responsibility to ensure the integrity of the data they use.

Each employee or potential data user will be given such information, instructions and training as is necessary in order to ensure that they are aware of their contractual responsibilities in relation to personal data and so that they are aware that they can, in some cases, be held personally responsible if any personal data is improperly disclosed, destroyed or obtained.

2. PROCEDURES

The Data Protection Officer has responsibility to co-ordinate the Authority's response to the Data Protection Act 1998 and the Freedom of Information Act 2000, to ensure that the provisions of the legislation are met. This role has been assigned to the post of Data Management Officer.

Planning and reviewing the Service's Data Protection Policy, Strategy and Procedures will be carried out by the Data Management Officer on a regular basis, not less than annually.

Each department and fire station will have a designated representative(s) to act as a point of liaison with the Data Management Officer.

The Data Controller will also monitor personal data kept at their particular station or department to ensure that such data is maintained in accordance with the principles of the Data Protection Act. However, this does not absolve individuals from their responsibility of ensuring that personal data is maintained in accordance with the principles detailed in 2.2 below.

An employee wishing to know personal data about themselves should contact Human Resources as per Standing Order 2/21 Personal Information Policy.

2.1 Scope of personal data

2.1.1 Personal data or information

- Any information held electronically (including all emails) or manually – which relates to a ***living*** individual who can be identified:
- from the information ;
- from the information combined with other information which is in the possession of the Service or is likely to come in to the possession of the Service; or
- includes any intentions or opinions the Service may have towards the individual.

2.1.2 Sensitive data

Staff have to be aware that the processing of sensitive information is limited to a small number of specified purposes, for example, the provision of health information to managers by the Occupational Health Centre to re-integrate long term sickness absentees back into the workplace.

The Data Protection Act defines sensitive data as;

- the racial or ethnic origin of the data subject;
- their political opinions;
- their religious beliefs or other beliefs of a similar nature;
- whether they are a member of a trade union;
- their physical or mental health condition;
- their sexual life; and
- any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

However, the Service does not keep or process all of this data, only that which it legitimately needs to or has obtained with the approval of a data subject.

For further specific guidance, see Standing Order 2/21, Personal Information Policy.

2.2 Principles of the Data Protection Act 1998

2.2.1 Principle 1 - fair processing

The Data Protection Act 1998 states that you cannot hold personal data unless you meet at least one criterion from Schedules 2 and 3 of the Act.

Schedules 2 and 3 are attached – Appendix 1

If you do not meet at least one criterion, you will be in breach of the Act.

Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:

- at least one of the conditions in **Schedule 2** is met; and
- in the case of sensitive personal data (defined in 2.1.2), at least one of the conditions in **Schedule 3** is also met.

Any activity whatsoever that involves personal information – held electronically or manually, such as obtaining, recording, holding, disseminating or making available the information, or carrying out any operation or set of operations on the information. It includes organising, adapting, amending and processing the information, retrieval, consultation, disclosure, erasure or destruction of the information. **It is difficult to envisage any activity which does not amount to processing and consideration should be given to conducting a Privacy Impact Assessment (PIA) when**

embarking on projects and/or activities that may involve processing personal data.

The PIA process is attached - Appendix 2.

If an organisation or individual holds any data that matches any of the above criteria, then they will have to legitimise why they are holding this data. An organisation or individual will also be in breach of the Act if it cannot legitimise the reason for holding the data even if it does match one of the criteria. If data controllers or data users are at all unsure regarding what is a legitimate reason for holding the data, they should seek the advice of the Data Protection Officer.

The processing of data for the purposes of carrying out of 'directed' and intrusive covert surveillance; the use of covert human intelligence sources; the interception of communications; and the acquisition and disclosure of communications data is covered under the Regulation of Investigatory Powers Act 2000 (RIPA).

The RIPA process is attached - Appendix 3.

2.2.2 Principle 2 - compatible purposes

Personal data shall be obtained for only one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

2.2.3 Principle 3 - extent of data

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

2.2.4 Principle 4 - data accuracy

Personal data shall be accurate and, where necessary, kept up to date.

2.2.5 Principle 5 - retention period

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or purposes. Some guidance about retention timescales exists in Standing Order 2/21 Personal Information Policy.

2.2.6 Principle 6 - data subject rights

Personal data shall be processed in accordance with the rights of data subjects under this Act. Data subjects include service users, employees including temporary and volunteers and those communities we serve.

The rights that are applicable to all data subjects are:

- the right to be informed that processing is being undertaken;
- the right to access personal data;
- the right to prevent processing in certain circumstances;
- the right to rectify, block or erase data; and
- the right to claim compensation for certain breaches of the Act.

2.2.7 Principle 7 - security and management of data

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss of, destruction of, or damage to personal data.

2.2.8 Principle 8 - foreign data transfer

Personal data shall not be transferred to a country or territory outside the European Community unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

2.3 Access to information

The Data Protection Act 1998 confers a right of access for data subjects to both computerised and manual data. This right of access depends on the way the data is kept, as access is available to 'structured filing systems'. The Act defines a relevant filing system as:

> 'Any set of information relating to individuals to the extent that, although the information is not structured by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals, or by reference to criteria relating to individuals, in such a way that particular information relating to a particular individual is readily accessible'. For example, Personal Record Files would be regarded as a 'structured filing system'.

Advances in technology have also impacted on how the Service processes personal information. E-mails are commonly used to transfer information about individuals **BUT** the same eight principles listed above are applicable, that is, the data subject has the right to know that information is being processed about them and also rights of access see 2.2.6 Principle 6.

The Data Protection Act requires that an organisation registers with the Information Commissioner's Office the types of information held about individuals, the reason for holding such information, and the circumstances in which that information will be used.

Certain personal information is recorded for Government purposes. However, the justification of recording identification details of living individuals should be established on every occasion.

The Service will notify the Information Commissioner of the purpose and processing details of this procedure.

2.3.1 Unincorporated clubs or associations

(Station Social Clubs, Sports and Welfare Associations and Benevolent Fund).

Such organisations were previously exempt from the Act, but must now comply, but are not required to register under the Data Protection Act 1998.

Whilst it is not necessary to notify the Information Commissioner of the personal data held, this does not exempt clubs from the first principle of the Act, that is, personal data shall be processed fairly and lawfully.

2.4 Requests for information

Departments or stations will have a nominated data controller. All requests for information in whatever form, for example, paper records, computer records, tapes, and so on, should be forwarded through the Internal Data Controller who will then liaise with the Data Management Officer.

If a request for information is received in a department, section or on a station it must be date stamped and forwarded immediately for the attention of the Data Management Officer, Data Management Section, marked 'Data Protection Request'. If possible, the information should be sent by e-mail.

The Data Management Officer will be responsible for recording the request, obtaining the information from the relevant department, charging any appropriate fees and ensuring that the request is answered within the timescale. The timescale for response to requests for information is 40 days and the suggested fee is £10 but this is not always charged.

Requests for the disclosure of personal data related to the 'Transfer of Undertakings (Protection of Employment) Regulations' (TUPE) 2006 are the responsibility of the Employee Relations team within the Human Resources Department.

The Data Management Officer will liaise with the data controller of the section, department or station concerned for assistance in providing the information requested.

It is imperative that information is provided in a timely manner to ensure that the specified timescales are met.

2.4.1 Requests for incident information

The Service is constantly receiving enquiries from solicitors, loss adjusters, insurance companies and other interested parties for details of fires and other Fire Service activities. The intentions of the enquirer are often unknown or liable to change at a later date.

The Service is not entitled to release information about a data subject to any third party without the data subject's consent; there are a few exceptions, for example, data requested by the police to assist them with criminal investigations. Fire Service reports, in particular the FDR1 Fire Report, contain information about persons involved in incidents and are therefore not to be released by fire stations.

All such requests must be submitted in writing by the party wishing to obtain the information. This is to be forwarded to the Data Management section in the Resources Directorate. Where necessary, Data Management will obtain the authority of the data subject before agreeing to any request for information.

A fee will usually be charged for this information.

2.4.2 Release of information for legal proceedings

When the Fire Authority is involved in legal proceedings, the Civil Procedure Rules require that all relevant documents shall be disclosed to the other parties involved. This includes all documents which are, **or have been** in the possession, custody or power of the relevant party and which relate to any matter in question between the parties.

Stringent time limits are imposed for disclosure of documentation. Hence it is vital that all documents are forwarded, as soon as possible after the request has been made.

A request for such documentation will usually be made by the Litigation Section to the relevant section, department or station. A thorough search must be made for all relevant documents.

All such documents, upon request, will be forwarded, as soon as practically possible, to the Litigation Section.

This request includes **all** relevant documents, including original or rough notes, and whether they are supportive or potentially damaging.

In general terms, it is likely that all available documentation is discloseable and therefore, personnel should forward all documents, which will be considered by the Authority's advisors before disclosure.

In certain circumstances, it may be necessary to forward original documents held. On such occasions, the requesting officer will determine whether new documentation is to be commenced, or whether original documents will be returned.

If original documents are forwarded, copies should be taken and preserved by the forwarding party.

Where copies of documents are forwarded, care must be taken to ensure the best possible quality copy is obtained.

2.4.3 Definition of documents (legal proceedings)

As all relevant documentation should be disclosed, it is not possible to provide a definitive list. However, for the purposes of this order, examples include: **all** paper records, written or printed, reports – including FDR1 and narratives (where provided), internal and external memoranda, accounts, invoices and contracts, any information held on computer or other mode of electronic storage, for example, e-mails, CD-ROM, diagrams, plans, maps, photographs and videos.

It should be noted that the marking of any discloseable document 'confidential' or 'personal' does not necessarily preclude disclosure in respect of legal proceedings.

The requirements of this standing order emphasise the importance of maintaining comprehensive and accurate filing systems, as the implications of non-disclosure of relevant documents are far reaching.

2.4.4 Requests for information from fire safety departments

Requests in respect of fire safety advice or information will be directed to the data controller of the nearest fire safety centre or Fire Safety Section of the Technical and Operational Support Directorate for action.

2.4.5 Information received or requested from the police about employees

On occasions, the Service has been contacted by police officers, who have either requested personal information about employees, or have notified the Service that employees have been arrested or involved in incidents to which the police have been called. Discussions with the police have indicated that the Fire Service is not a 'notifiable occupation' for disclosing convictions of persons for certain employers.

Therefore, the following procedure will be adopted upon receipt of such requests from the police, or where information is received about individual employees:

- where the police request information from a station, the officer in charge should only confirm whether or not an individual is employed at the station;
- any requests for further information about employees should be refused and the requesting police officer referred to the duty principal command officer via Fire Control. The Service will then only release personal details where a serious crime is being investigated or where a warrant has been issued;
- given that all employees are obliged to notify the Service if they have been charged with a criminal offence, senior officers should no longer visit police stations if informed by the police that an individual has been detained or questioned whilst off duty. The Service does provide welfare support should individuals require it;
- personnel who are being questioned or detained by the Police and who would be unable to report for duty as a result, should request the police to contact Fire Control and inform the duty officer that they will be unable to attend for duty. The duty principal command officer will then be informed and will take appropriate action; and
- requests from the police for copies of tapes from Fire Control will be managed and actioned by Fire Control. The procedure is detailed in Fire Control.

2.5 Complaints

Any complaints must be submitted through the Customer Care and Compliments, Comments and Complaints procedure.

2.6 Important legislation to consider

The Freedom of Information Act 2000 (see Standing Order 1/5) and the Environmental Information Regulations 2004 (see Standing Order 1/10) enable individuals to request access to information held by the Service. Both sets of legislation aim to encourage more open and accountable government by establishing a general statutory right of access to official records and information held by public authorities. This compliments and is influenced by the Data Protection Act 1998, as generally information which involves, or can identify an individual is exempt; however, there may be requests for information, which will only in part identify an individual. Similarly, a request may refer to individuals, but in the majority may relate to information held which can be provided. Therefore, any request for information needs to take into consideration the requirements of all three pieces of legislation. All requests of this nature must be

forwarded to the Data Management Officer at Fire Service Headquarters who will establish what legislation any request may come under, and provide a formal response.

2.7 Further information

Further information or clarifications can be obtained from the Data Management Officer, telephone number 0121 380 6535.

3. CROSS REFERENCES

Standing Order 1/5 – Freedom of Information Act 2000

Standing Order 1/10 – Environmental Information Regulations 2004

Standing Order 1/17 – Re-use of Public Sector Information Regulations 2005

Standing Order 2/21 – Personal Information Policy

Standing Order 21/1 – Customer Care and Compliments, Comments and Complaints (CCC Policies)

4. KEY CONSULTEES

Operations Commander Birmingham North

Station Commander Woodgate Valley

Station Commander Bournbrook

Station Commander Canley

Station Commander Bickenhill

Station Commander Solihull

Ladywood Red Watch

Walsall White Watch

Handsworth Green Watch

Coventry Blue Watch

Brierley Hill Purple Watch

Human Resources Employee Relations Manager

Group Commander B FiReControl and Firelink Project

Equality and Diversity

Integrated Risk Management Team

Safety, Health and Environmental Team

Fire Brigades' Union

Fire Officers' Association

UNISON

Chief's Policy Advisor

Word Processing Unit

5. EQUALITY IMPACT ASSESSMENT

6. OWNERSHIP

The preliminary impact assessment screening raised issues which were dealt with by a full impact assessment.

This Standing Order did not require Corporate Board or Authority approval.

7. RESPONSIBILITY AND REVIEW/AMENDMENT

7.1 Responsible Corporate Board Member/Department

Director, Resources/Data Management.

7.2 Created/fully reviewed/amended

This Order has been reviewed by the Data Management Officer in January 2011 and Appendix 2 has been inserted by HR Employee Relations in November 2011.

Reviewed and amended November 2012.

Reviewed and amended May 2013.

APPENDIX 1

1. Schedule 2 Conditions (Data Protection Act 1998)

Schedules 2 and 3 set out specific conditions that have to be met before processing of personal data can take place; these relate to the first of the 8 principles. The conditions are different for sensitive data and non-sensitive data.

Broadly, **non-sensitive data** is not to be processed unless at least **one** of the following conditions has been met:

- the data subject has given their consent to the processing;
- the processing is **necessary** for the performance of a contract to which the data subject is party (the employment contract), or for taking steps to enter into such a contract;
- the Data Controller has to process the information in order to comply with non-contractual legal obligations (such as health and safety obligations);
- the processing is **necessary** to protect the vital interests of the data subject;
- the processing is **necessary** for the administration of justice, exercise of crown functions, or the exercise of any other functions of a public nature exercised in the public interest; or
- the processing is **necessary** for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data is disclosed, except where the processing is unwarranted in any particular case because of prejudice to the rights and freedoms or legitimate interests of the data subject. The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.

2. Schedule 3 Conditions (Data Protection Act 1998)

In the case of sensitive data, processing is permitted only if at least one of the following conditions is met:

- the data is of sensitive personal nature consisting of information as to racial or ethnic origin;
- the individual has given their explicit consent to the processing;
- the processing is necessary for the purposes of exercising or performing any right conferred or obligation imposed by law on the Data Controller in connection with employment;
- the processing is necessary to protect the vital interests of the individual in a case where either the consent cannot be given (incapacity, for example) or else the Data Controller cannot reasonably be expected to obtain consent (for example, the individual cannot be contacted despite various attempts over a considerable length of time);
- the processing is carried out in the course of its legitimate activities by any body or association not established for profit and which exists for political, philosophical or trade union purposes, and which relates only to individuals who are members of that body;
- the individual has already made the information public, by taking deliberate steps;
- the processing is necessary for the purpose of or in connection with legal proceedings, obtaining legal advice or establishing or exercising or defending legal rights;

- the processing is necessary for the administration of justice or exercise of crown functions;
- the processing is necessary for medical purposes and is undertaken by a health professional; or
- the personal data are processed in circumstances specified in an order made by the Secretary of State.

APPENDIX 2

PRIVACY IMPACT ASSESSMENTS (PIA)

1. Introduction

1.1 PIAs are used as a systematic way to assess all policies, procedures, activities and proposed projects for impact on the privacy of employees of the West Midlands Fire Service and members of the public. PIAs are similar to Equality Impact Assessments (EIA) and there is not a legislative requirement to undertake them within the Fire and Rescue Service but they are mandatory within central government. It is a suggested methodology of assessing the privacy risks associated with new projects or initiatives and what steps can be taken to mitigate the risk.

1.2 The methodology is issued by the Information Commissioner's Office, the overarching body for the regulation of data protection and associated areas. PIAs are intrinsically linked to data protection and provide some good practice surrounding the areas where an organisation may be vulnerable when processing personal data.

1.3 There are some aspects of data sharing that are governed by separate legislation which may also need to be considered during the PIA process, for example, Crime and Disorder Act 1998.

1.4 There are no consequences for not undertaking PIAs but if a data breach occurs and the methodology is not used, then the likelihood is that greater fines and harsher enforcement action could be taken against the organisation.

2. The meaning of privacy

In its brodest term privacy is about the integrity of the individual. It therefore encompasses many aspects of the individual's social needs.

2.1 There are four aspects that are commonly used to assess the impact on privacy:-

2.1.1 The privacy of personal information:

individuals generally do not want data about themselves to be automatically available to other individuals and organisations.

2.1.2 The privacy of the person:

this is sometimes referred to as 'bodily privacy' and is concerned with the integrity of the individual's body, for example, compulsory immunisation or compulsory provision of samples of body fluid and tissue.

2.1.3 The privacy of personal behaviour:

this relates to the observation of what individuals do, and includes such issues as optical surveillance and 'media privacy', for example, CCTV.

2.1.4 The privacy of personal communications:

this relate to the freedom that individuals have to communicate amongst themselves, using various media, without routine monitoring of their communications by other persons or organisations.

Any new policy development, activity, service project or any policies being amended and reviewed should undergo a PIA. The aim of a PIA is to highlight the likely impact of the policy, activity or project on the four common aspects of privacy listed above. It will also determine the extent of any differential impact and identify ways in which the policy should be changed or this impact mitigated if adverse.

The assessment process requires policy leads to demonstrate that a number of key considerations surrounding privacy have been taken into account in developing or revising a policy or practice.

3. Reasons for undertaking a PIA

- Identifying and managing risks
- Avoiding unnecessary costs
- Inadequate solutions
- Avoiding loss of trust and reputation
- Informing the organisation's communication strategy

4. The outcomes of a successful PIA

The outcomes of an effective PIA are:

- the identification of the policy, activity or project's privacy impacts;
- appreciation of those impacts from the perspectives of all stakeholders;
- an understanding of the acceptability of the project and its features by the organisations and people that will be affected by it;
- identification and assessment of less privacy-invasive alternatives;
- identification of ways in which negative impacts on privacy can be avoided;
- identification of ways to lessen negative impacts on privacy;
- where negative impacts on privacy are unavoidable, clarity as to the business need that justifies them; and
- documentation and publication of the outcomes.

5. Purpose

If the policy, project, activity has a significant impact on the privacy of people then a full **PIA must be completed.**

A full PIA is **not** likely to be required when:

- there are no concerns of adverse impact but a data compliance check should be undertaken to ensure compliance with the Data Protection Act 1998

A small-scale PIA is **likely to be** required when:

- there may be some concern or evidence of negative or adverse impact. An example of this is the application of existing personal data to a new purpose

A full PIA **will be** required when:

- there is substantial concern or evidence of negative or adverse impact. An example of this would be compulsory substance testing for all employees.

6. Who is responsible for carrying out PIAs?

The lead person on any policy formation, new project or review is responsible for making sure that an initial PIA which may lead to a small-scale or full PIA is completed, if required. This may be undertaken at the same time as an Equality Impact Assessment (EIA) as both assess impacts on people whether they are employees or service users.

The person responsible for completing the PIA has the responsibility to make sure that the Data Management Officer is provided with **electronic copies** of the full PIA in addition to maintaining a file of the original documentation and supporting evidence.

The Data Management Officer can provide advice guidance and assistance when requested.

7. Initial PIA screening process

At the screening stage, members of staff responsible for completing PIAs will need to identify whether the policy, activity, function or project impacts directly on the privacy of employees or members of the public and make an informed and clearly justifiable decision based on the analysis of data as to whether an activity requires a PIA and if so whether it is a small-scale or full PIA.

PIAs are one way in which an organisation can design privacy into its policy and procedures and meet their obligations under the Data Protection Act 1998 and the Human Rights Act 2000. Proportionality is a key principle and the scale of the PIA should reflect this.

The following aspects should be considered.

Scope and timescales for project or activity (including review date)

Detail how long this policy, activity or project is expected to run or how long it will take to implement. Also state the expected time scale when you expect to review the activity and any impacts on privacy.

Outline of main aims of this activity, policy or project

Be specific, what are the intended outcomes of your activity? How do you plan to achieve them?

Who will benefit or be affected by this policy or activity?

Will your activity affect staff and/or service users? Who is it intended to benefit? Who could it affect? It is not enough to put that it will affect all service users.

(a) Service users and community?

Will the activity affect different groups differently? Do you have any data on this if it is an existing strategy? Consider direct impacts and less obvious indirect impact. What are the demographics of the service users it will affect? If you do not have any data you cannot make an informed decision which you may later have to justify. If you have little data and a differential impact is likely or possible then you should consider a full or small-scale PIA.

(b) WMFS employees?

How many staff could it affect, both directly and indirectly? Do you have data on the make up of the staff affected. (Will it affect job roles? Working locations?)

Requirement for PIA and level required

This section must include the decision about the PIA requirement and justification as to whether the outcome is 'PIA not required'. 'Small-scale PIA' or 'Full PIA'.

You must justify your decision as to whether a full PIA is needed or not, consider:

- proportionality;
- the actual or potential impact; and
- data you have gathered, or any previous data available.

The completed initial PIA is then sent to the Data Management team who will review and get back to you within 12 working days

8. Conducting a PIA

Once the level of PIA has been determined, the process for completing a PIA for any project needs to reflect the nature of the project (for example, new system, replacement system, enhancements to an existing system, new technology, outsourcing, changed business processes or staff instructions, replacement user interface, revised privacy policy statement, drafting of legislative changes).

There are 5 suggested phases and these need not be formalised.

- preliminary phase;
- preparation phase;
- consultation and analysis phase(s);
- documentation phase; and
- review and audit phase.

8.1 Preliminary phase

The preliminary phase should have as deliverables, a project outline, a preliminary assessment of privacy concerns and some preliminary talks with key stakeholders.

8.2 Preparation phase

In this phase, organisations may undertake a stakeholder analysis, development of a consultation strategy and plan. Due to the nature of a small-scale PIA, these tasks do not need to be formalised.

8.3 Consultation and analysis phase(s)

This includes consultations with stakeholders, risk analysis, the articulation of problems and the search for constructive solutions.

Consultation does not have to be a formal process and can be limited to the stakeholders who have a key interest in the project or those who may have the biggest concerns about the project.

The key deliverable is a document (such as a privacy design features paper or a meeting outcomes report) that details the privacy impacts identified and the solutions or actions which will be taken to deal with them.

8.4 Documentation phase

The purpose of the documentation phase is to document the process and the outcomes. The deliverable is a PIA Report, which may draw heavily on the document produced during the consultation and analysis phase. Depending on the context, this might be a relatively brief 'note to file', with copies to relevant parties; but circumstances may justify a more carefully prepared document.

8.5 Review and audit phase

The purpose of this phase is to ensure that the design features arising from the PIA are implemented and are effective. The deliverable is a review or update report. Once again, in some contexts a 'note to file', with copies distributed to relevant parties, might be sufficient to achieve this requirement. In other cases, a more detailed document may be required.

9. Monitoring

The PIA of the policy and the consultation on it, will have helped to anticipate its likely effects on the privacy of individuals or specific groups of people. Therefore monitoring of the policy once it is in operation **must** be undertaken.

The final policy may be revised to take account of some or all of these findings, but the actual impact of the policy will only be known once it is in operation.

10. Publication

All policy owners are responsible for ensuring that a full PIA is completed and sent **electronically** to the Data Management Section. A copy of the policy must also be attached to the PIA documentation.

The full reports will be made available on the Data Management intranet site and brief summary reports published on the WMFS internet site. The full reports will also be made readily available to anyone who requests a copy and arrangements will be made

to provide the results of PIAs in alternative languages and alternative formats as and when requested.

Criteria for small-scale PIA

This section provides guidance for evaluating whether a small-scale PIA should be conducted.

The evaluation depends on sufficient information about the policy, activity or project having been collected when preparing for the PIA screening process. The evaluation process involves answering a set of questions about characteristics of the project or the system that the project will deliver.

The 15 questions about project characteristics

Technology

(1) Does the project involve new or inherently privacy-invasive technologies?

Examples of such technologies include, but are not limited to, smart cards, radio frequency identification (RFID) tags, biometrics, locator technologies (including mobile phone location, applications of global positioning systems (GPS) and intelligent transportation systems), visual surveillance, digital image and video recording, profiling, data mining, and logging of electronic traffic.

Justification

(2) Is the justification for the new data-handling unclear or unpublished?

Individuals are generally much more accepting of measures, even measures that are somewhat privacy-intrusive, if they can see that the loss of privacy is balanced by some other benefits to themselves or society as a whole.

Identity

An identifier enables an organisation to collate data about an individual and identifiers are used for multiple purposes to enable data consolidation. Increasingly onerous registration processes and document production requirements imposed are warning signs of potential privacy risks.

(3) Does the project involve an additional use of an existing identifier?

(4) Does the project involve use of a new identifier for multiple purposes?

(5) Does the project involve new or substantially changed identity authentication requirements that may be intrusive or onerous?

Data

(6) Will the project result in the handling of a significant amount of new data about each person, or significant change in existing data-holdings?

(7) Will the project result in the handling of new data about a significant number of people, or a significant change in the population coverage?

(8) Does the project involve new linkage of personal data with data in other collections, or significant change in data linkages?

The degree of concern about a policy, activity or project is higher where data is transferred out of its original context. The term 'linkage' encompasses many kinds of activities, such as the transfer of data, the consolidation of data-holdings, the storage, amalgamation and matching of personal data from multiple sources.

Data handling

(9) Does the project involve new or changed data collection policies or practices that may be unclear or intrusive?

(10) Does the project involve new or changed data quality assurance processes and standards that may be unclear or unsatisfactory?

(11) Does the project involve new or changed data security arrangements that may be unclear or unsatisfactory?

(12) Does the project involve new or changed data access or disclosure arrangements that may be unclear or permissive?

(13) Does the project involve new or changed data retention arrangements that may be unclear or extensive?

(14) Does the project involve changing the medium of disclosure for publicly available information in such a way that the data becomes more readily accessible than before?

Exemptions

(15) Will the project give rise to new or changed data-handling that is in any way exempt from legislative privacy protections?

Perspectives to consider

As with the criteria for full-scale PIA, risks may be overlooked unless these questions are considered from the various perspectives of each of the stakeholder groups, rather than just from the viewpoint of the deaprtment or section that is conducting the policy, activity or project.

Applying the criteria

Where the answers to questions are "Yes", consideration should be given to the extent of the privacy impact and the resulting risk to the policy, activity or project. The greater the significance, the more likely that a small-scale PIA is warranted.

Full PIA assessment guidance notes

Step 1 – Criteria for full-scale PIA

This section provides guidance for evaluating whether a full-scale PIA should be conducted. The evaluation depends on sufficient information about the policy, activity or project having been collected during the previous step.

The evaluation process involves answering the following set of 11 questions about key characteristics of the project and the system that the project will deliver.

The answers to the questions need to be considered as a whole, in order to decide whether the overall impact and the related risk, warrant investment in a full-scale PIA.

The 11 questions about key characteristics of the policy, activity or project

Technology

(1) Does the policy, activity or project apply new or additional information technologies that have substantial potential for privacy intrusion?

Examples include, but are not limited to, smart cards, radio frequency identification (RFID) tags, biometrics, locator technologies (including mobile phone location, applications of global positioning systems (GPS) and intelligent transportation systems), visual surveillance, digital image and video recording, profiling, data mining, and logging of electronic traffic.

Identity

(2) Does the project involve creating new ways to identify people, for example, identifiers, re-use of existing identifiers, or intrusive identification, identity authentication or identity management processes?

Examples of relevant policy, activity or project features include a digital signature initiative, a multi-purpose identifier, interviews and the presentation of identity documents as part of a registration scheme and an intrusive identifier such as biometrics.

(3) Might the project have the effect of denying anonymity and pseudonymity, or converting transactions that could previously be conducted anonymously or pseudonymously into identified transactions?

Many functions cannot be effectively performed without access to the individual's identity and some others do not require identity. An important aspect of privacy protection is sustaining the right to interact with organisations without declaring one's identity.

Multiple organisations

(4) Does the project involve multiple organisations, whether they are government agencies (for exampe, in 'joined-up government' initiatives) or private sector organisations (for example, as outsourced service providers or as 'business partners')?

Schemes of this nature often involve the breakdown of personal data silos and identity silos and may raise questions about how to comply with data protection legislation. This breakdown may be desirable for fraud detection and prevention and in some cases for business process efficiency. However, data silos and identity silos have in many cases provided effective privacy protection.

Data

(5) Does the policy, activity or project involve new or significantly changed handling of personal data that is of particular concern to individuals?

The Data Protection Act identifies a number of categories of 'sensitive personal data' that require special care. These include racial and ethnic origin, political opinions, religious beliefs, trade union membership, health conditions, sexual life, offences and court proceedings.

There are other categories of personal data that may give rise to concerns, including financial data, particular data about vulnerable individuals, and data which can enable identity theft.

Further important examples apply in particular circumstances. The addresses and phone-numbers of a small proportion of the population need to be suppressed, at least at particular times in their lives, because such **'persons at risk'** may suffer physical harm if they are found.

(6) Does the project involve new or significantly changed handling of a considerable amount of personal data about each individual in the database?

Examples include intensive data processing such as welfare administration, healthcare, consumer credit, and consumer marketing based on intensive profiles.

(7) Does the policy, activity or project involve new or significantly changed handling of personal data about a large number of individuals?

Any data processing of this nature is attractive to organisations and individuals seeking to locate people, or to build or enhance profiles of them.

(8) Does the policy, activity or project involve new or significantly changed consolidation, inter-linking, cross-referencing or matching of personal data from multiple sources?

This is an especially important factor. Issues arise in relation to data quality, the diverse meanings of superficially similar data-items, and the retention of data beyond the very short term.

Exemptions and exceptions

(9) Does the policy, activity or project relate to data processing which is in any way exempt from legislative privacy protections?

Examples include law enforcement and national security information systems.

(10) Does the policy, activity or project's justification include significant contributions to public security measures?

Measures to address concerns about critical infrastructure and the physical safety of the population usually have a substantial impact on privacy. This may result in tensions with privacy interests, and create the risk of opposition and non-adoption of the programme or scheme.

(11) Does the policy, activity or project involve systematic disclosure of personal data to, or access by, third parties that are not subject to comparable privacy regulation?

Disclosure may arise through various mechanisms such as sale, exchange, unprotected publication in hard-copy or electronically-accessible form, or outsourcing of aspects of the data-handling to sub-contractors.

Third parties may not be subject to comparable privacy regulation because they are not subject to the provisions of the Data Protection Act or other relevant statutory provisions

Perspectives to consider

It is important to appreciate that the various stakeholder groups may have different perspectives on these factors. If the analysis is undertaken solely from the viewpoint of the organisation itself, it is likely that risks will be overlooked. It is therefore recommended that stakeholder perspectives are also considered as each question is answered.

Applying the criteria

Once each of the 11 questions has been answered individually, the set of answers needs to be considered as a whole, in order to reach a conclusion as to whether a full-scale PIA is warranted. If it is, a conclusion is also needed as to whether the scope of the PIA should be wide-ranging, or focused on particular aspects of the policy, activity or project.

APPENDIX 3

REGULATION OF INVESTIGATORY POWERS ACT 2000
POLICY FOR SURVEILLANCE, A COVERT HUMAN INTELLIGENCE SOURCES AND THE ACQUISITION OF COMMUNICATIONS DATA
(See 2.4 of main order 2/16)

REGULATION OF INVESTIGATORY POWERS ACT 2000
POLICY FOR SURVEILLANCE, COVERT HUMAN INTELLIGENCE SOURCES AND THE ACQUISITION OF COMMUNICATIONS DATA

1. Introduction

1.1 The Regulation of Investigatory Powers Act 2000 (RIPA) provides a framework for control and supervision of investigatory powers exercised by public bodies, including local authorities, in order to balance the need to protect privacy of individuals with the need to protect others, particularly in light of the Human Rights Act 1998. RIPA provides a statutory basis for the authorisation and use by the security and intelligence agencies, law enforcement and other public authorities, of covert surveillance, agents, informants and undercover officers. It regulates the use of these techniques and safeguards the public from unnecessary invasions of their privacy.

1.2 RIPA covers the carrying out of 'directed' and intrusive covert surveillance; the use of covert human intelligence sources; the interception of communications; and the acquisition and disclosure of communications data. RIPA also provides for the appointment of independent Surveillance Commissioners who will oversee the exercise by public authorities of their powers and duties.

1.3 Of conceivable relevance to the work of the Service are the provisions of Part ll of RIPA that cover the use and authorisation of 'directed' surveillance (section 28) and covert human intelligence sources (section 29) by public authorities. Part ll of RIPA provides for a new authorisation mechanism which authorities undertaking covert surveillance must use.

1.4 It may occasionally be necessary for officers to use covert surveillance techniques for the following reasons:

- audit investigation;
- community safety;
- health and safety compliance;
- environmental protection and pollution control;
- potential fraudulent activities; and
- employee terms and conditions compliance.

This list is not necessarily exhaustive.

1.5 This policy addresses solely issues having relevance to the activities of the Service and how the authorisation mechanisms required by the Act will be administered.

1.6 In addition, the investigatory powers will be exercised by the Service in compliance with the Codes of Practice contained in:-

- the Regulation of Investigatory Powers (Covert Human Intelligence Sources: Code of Practice) Order 2002 (SI 2002/1932);
- the Regulation of Investigatory Powers (Covert Surveillance: Code of Practice) Order 2002 (SI 2002/1933); and
- the Regulation of Investigatory Powers (Communications Data) Order 2003: Home Office Draft Code of Practice entitled '*Accessing Communications Data'*.

2. The meaning of 'surveillance' within the Act

2.1 Covert 'directed' surveillance is covered by RIPA.

Surveillance is 'directed' when it is undertaken in relation to a specific investigation or a specific operation which is likely to result in the obtaining of private information about a person.

Surveillance is covert where it is carried out in a manner calculated to ensure that the person or persons subject to the surveillance are unaware that it is or may be taking place.

Such forms of surveillance involve observing an individual or group of people whether through unaided observation or listening or through the use of technical devices and when information regarding their private or family lives is likely to be obtained.

2.2 Special provisions apply where information enjoying legal privilege or certain types of confidentiality may be obtained. In such circumstances, which are not expected to be relevant to the Authority's activities, the approval of the Information Commissioner or the Authority's head of paid service is required.

3. The meaning of 'covert human intelligence sources' (CHIS) within the Act

3.1 When person A establishes, maintains or uses a relationship (personal or otherwise) with person B for information gathering purposes or uses, or discloses information obtained by such a relationship, or arising from it, and s/he does so when B is unaware that it is or may be happening, then person A is a Covert Human Intelligence Source.

4. The meaning of 'communications data' within the Act

4.1 Communications data is information held by communications service providers relating to communications made by their customers. This includes itemised call records, routing information and subscriber details. Communications data does not include the actual content of any communications.

4.2 The Service in acquiring this data must ensure that it is required either (1) in the interests of public safety, or (2) in preventing or detecting crime. Additionally, this information must be proportionate to what is sought to be achieved. In practical terms, this would cover such things as:-

- during a fire investigation, obtaining contact details in order to speak to whoever reported the fire to help piece together the sequence of events; or
- to investigate hoax or malicious calls.

4.3 It should be noted that the Act has no impact on the existing protocols relating to requests for data when responding to an emergency (999/112) call where the caller has cleared the line before giving adequate details about the location at which an attendance is required. These requests will continue to be dealt with under the Data Protection Act and in accordance with the procedures set out in the '*Code of Practice for the Public Emergency Call Services between Public Network Operators and the Emergency Services'.*

5. Authorisation - CHIS and 'directed' surveillance

5.1 The Service will apply a procedure for the proper authorisation and recording of its activities and for the use of CHIS in accordance with the Act.

5.2 The Service shall ensure that officers with responsibility for authorising the acquisition of communications data or carrying out surveillance and the use of CHIS shall be made aware of their obligations to comply with the Act and with this policy. Furthermore officers shall receive appropriate training or be appropriately supervised in order to carry out functions under the Act. In particular, all officers with responsibilities under the Act will be familiar with the Codes of Practice referred to above, so far as they relate to their responsibilities.

5.3 To ensure that these powers are used appropriately, authority for authorisation for surveillance or CHIS will be obtained from the Director of Human Resources or, if not available, the Duty Principal Officer prior to commencement. Forms of Authorisation can be obtained from the Litigation Officer.

6. Review of authorisations and policy - CHIS and 'directed' surveillance

6.1 The Service will ensure that authorisations for surveillance or CHIS, once granted, are reviewed on a monthly basis and are renewed or cancelled as appropriate.

6.2 This policy and accompanying procedure shall be reviewed from time to time in light of changes in legislation, case law, or for the better performance of the procedure.

6.3 To provide an independent overview of Service activity, a half-yearly report will be provided to the Fire Authority by the Monitoring Officer. The information that will be given to the Fire Authority will be based on usage numbers only.

7. Procedure for surveillance - CHIS and 'directed' surveillance

7.1 When a member of the Service believes that it is necessary for surveillance ('directed' or CHIS) to be undertaken to enable the gathering of information, they should, in the first instance, discuss their request confidentially with the Litigation Officer. The Director of Human Resources, (referred to as the Authorising Officer), or, in his absence, the Duty Principal Officer will then authorise the request for surveillance to be undertaken.

7.2 Assuming that outline agreement is reached, then the officer initiating the request must complete and forward the form RIPA 1 'Application for the authorisation of 'directed' surveillance or RIPA 5 'Application for the authorisation of covert human intelligence source (CHIS)' to the Authorising Officer under private and confidential cover.

7.3 On receipt, the Authorising Officer will ensure that the application is provided with a reference number obtained from the Human Resources database and that the details are typed onto the Service's RIPA database held by the Human Resources Department for entry onto the appropriate register file.

7.4 **Authorisations must only be granted for one month and then reviewed.**

7.5 The Authorising Officer will discuss the position with the officer making the original request, forwarding the appropriate forms for completion and return before the renewal date arrives.

7.6 Details of the completed forms and renewal date will be entered onto the Service's RIPA database by the Human Resources Department.

7.7 **Renewal of authorisations must only be granted twice.**

7.8 Surveillance can only be undertaken for a maximum of three months. If any further extensions of time are considered necessary, then the case must be discussed in detail with the Litigation Advisor or the Director of Human Resources.

8. Report to Corporate Board

Every six months, the litigation advisor is to provide Corporate Board with details of any surveillance which has been authorised under this legislation.

The information that will be submitted to Corporate Board will be details of usage numbers and reasons. No personal information will be released.

Agenda Item No.

WEST MIDLANDS FIRE AND RESCUE AUTHORITY

AUDIT COMMITTEE

6 JUNE 2016

1. CORPORATE RISK UPDATE

Report of the Chief Fire Officer.

RECOMMENDED

1.1 THAT Audit Committee approve the changes to the Corporate Risk Standing Order number 22/7 at Appendix 1.

1.2 THAT Audit Committee note and discuss the Audit Committee Corporate Risk Briefing at Appendix 2.

2. PURPOSE OF REPORT

2.1 This report is submitted to request Member approval of the revised Corporate Risk Standing Order following changes to the Corporate Risk reporting process, which were approved by Audit Committee on the 11th April 2016.

2.2 As part of these changes the Audit Committee will receive 'Audit Committee Briefings' which will focus on a particular risk or risks, this may include a risk where there has been a change in the overall risk rating. This provides the Audit Committee with the opportunity to engage in and influence more open discussion regarding how the risk is being managed. A Corporate Risk briefing has been included as an appendix to this report for discussion by the Audit Committee. This briefing focuses on Corporate Risk 11.

3. BACKGROUND

3.1 On the 11th April 2016 the Audit Committee approved to change the frequency of corporate risk reporting from four times to two times per municipal year.

However to ensure that Members are made aware of any significant changes to its corporate risks in a timely and effective way, it was also approved that the Audit Committee will be provided with regular updates upon specific risk issues as and when they emerge in the organisation. This approach will promote and enable Members to become more aware of specific risk critical issues in a timely way. It will also provide the opportunity for Members to discuss, critically challenge, shape and influence how the Service manages and controls its specific risks. Through this engaging and involving, Members will build their capability and understanding around risk management and will be provided with assurance as to the Service's arrangements for managing specific risks.

3.5 To support the implementation of this new approach across the Service, the Corporate Risk Standing Order 22/7 has been updated to reflect these changes and the changes being made internally to support the new approach. The revised Standing Order is set out in Appendix 1.

3.6 As part of this new approach a Corporate Risk Audit Committee Briefing has been included in this report for Member discussion. The Briefing focuses on Corporate Risk 11.

3.7 A further review of the current Corporate Risks is been carried out by officers. This review will consider if all of the risks are fit for purpose and current. Any proposed changes will be reported back to the Audit Committee at its meeting on 5 September 2016.

4. EQUALITY IMPACT ASSESSMENT

In preparing this report an initial Equality Impact Assessment is not required and has not been carried out. The matters contained in this report do not relate to a policy change.

5. LEGAL IMPLICATIONS

There are no legal implications associated with the implementation of the recommendations set out in this report.

6. **FINANCIAL IMPLICATIONS**

There are no financial implications associated with the implementation of the recommendations set out in this report.

7. **ENVIRONMENTAL IMPLICATIONS**

None

BACKGROUND PAPERS

Frequency of Risk Reporting to Audit Committee, Audit Committee Report, 11th April 2016.

The Author of this report is Deputy Chief Fire Officer Philip Hales, telephone number 0121 380 6004.

PHIL LOACH
CHIEF FIRE OFFICER

Ref. AU/AC/2016/June/125051614

WEST MIDLANDS FIRE SERVICE
CORPORATE RISK MANAGEMENT

1. STRATEGY

It is the strategy of the West Midlands Fire and Rescue Authority to have in place a structured risk management framework which supports the assessment and treatment of its corporate risks, as it is recognised that such a strategy will support the Fire and Rescue Authority in achieving its vision of 'Making West Midlands safer, stronger and healthier'. Effective risk management forms a key aspect of the corporate governance arrangements.

2. PROCEDURES

2.1 Definition of risk management

Risk management is the process of identifying threats and opportunities, evaluating their potential consequences and then determining the most effective and efficient methods of controlling and/or responding to them.

~~Whilst in the broadest context, risk management is the responsibility of every member of the Service, there are a number of sections that have responsibility for the management of risk such as the:~~

- ~~Strategic Planning, Improvement and Risk Team (SPIRiT), supporting the management of foreseeable corporate and strategic risk and embedding risk management within the organisation. Through the application of integrated risk management (IRM) methodology SPIRiT also supports the strategic assessment of risks in our community and influences the activity undertaken to reduce existing and potential risks. The Programme Support Office is responsible for ensuring a systematic and consistent approach to managing, recording, updating and reporting risks within the programme and project environment.~~

  ~~Note: The arrangements detailed above are subject to any changes made through the review of SPIRiT.~~

- ~~Safety, Health and the Environment Team, supporting the assessment and control of risks affecting the safety, health and welfare of those employed by the Authority or who are under its duty of care.~~

- ~~Emergency Response Planning Team, supporting the assessment of, and planning for risks associated with terrorist activity, significant environmental events and other emergencies.~~

- ~~Human Resources function, supporting the management of risk through effective planning, delivery of appropriate learning and development strategies, and formal engagement and consultation mechanisms that enable for sufficient numbers of appropriately skilled, competent and motivated employees.~~

- ~~In respect of the management of risk at operational incidents, the Service recognises that its personnel will be confronted by risks from a wide range of hazards. The roles and responsibilities for managing risk at incidents are set out in Operational Guidance – Incident Command, and other supporting documents cross referenced in that OPN. The Service sets out in its Operational Procedure Notes, Standing Orders and other guidance the systems, structures, frameworks, processes and procedures in place to enable for the effective management of risk at operational incidents.~~

2.2 The benefits of risk management

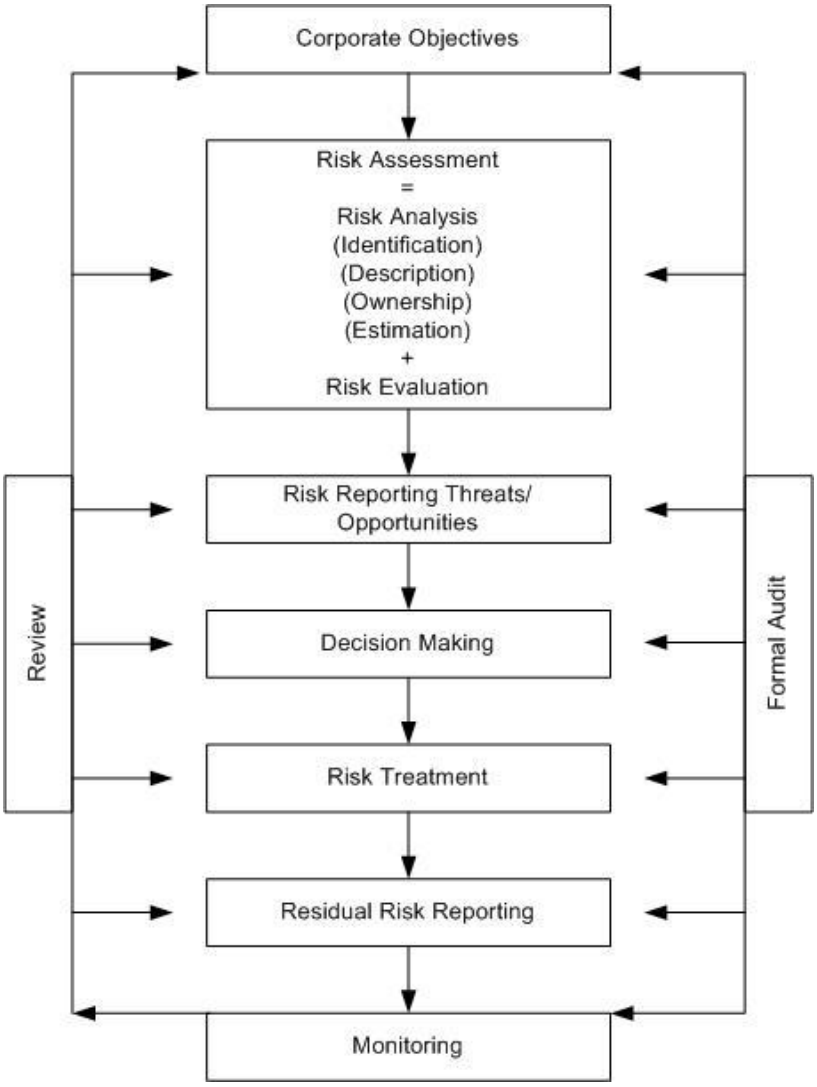
An effective risk management framework will deliver a wide range of benefits throughout all areas and levels of the organisation; in particular it will enable the Authority to deliver its

core functions of preventing, protecting and responding, meet its statutory duties and obligations, safeguard its reputation within the wider community and demonstrate its ability to deliver value for money. The benefits of an effective risk management framework include improved:

- Corporate management, through:
  - Informed decision making based on risk identification, analysis, control and monitoring, enabling the allocation of appropriately skilled, competent and motivated employees and resources to those areas of greatest risk;
  - Informed selection of strategic objectives, outcomes and targets based on risk identification, analysis, control and monitoring;
  - Improved ability to deliver against realistic and achievable strategic objectives, outcomes and targets through the provision of sufficient numbers of skilled, competent and motivated employees and resources; and
  - An improved performance management framework.
- Financial management, through:
  - Improved financial control arising from risk identification, analysis, control and monitoring; and
  - Reduction in financial costs associated with losses due to service interruption, litigation or insufficient and/or ineffective employees and so on.
- Customer focus, through:
  - Improved internal and external reputation arising from all the above; and
  - Reduction in service disruption arising from all the above.

2.3 The risk management framework

The risk management framework adopted by the organisation is based upon a simple, but effective, model which demonstrates how the principles of risk management can be achieved. This framework model is represented in Figure 1.


Corporate Objectives
Risk Assessment
=
Risk Analysis
(Identification)
(Description)
(Ownership)
(Estimation)
+
Risk Evaluation
Risk Reporting Threats/
Opportunities
Decision Making
Risk Treatment
Residual Risk Reporting
Monitoring
Review
Formal Audit

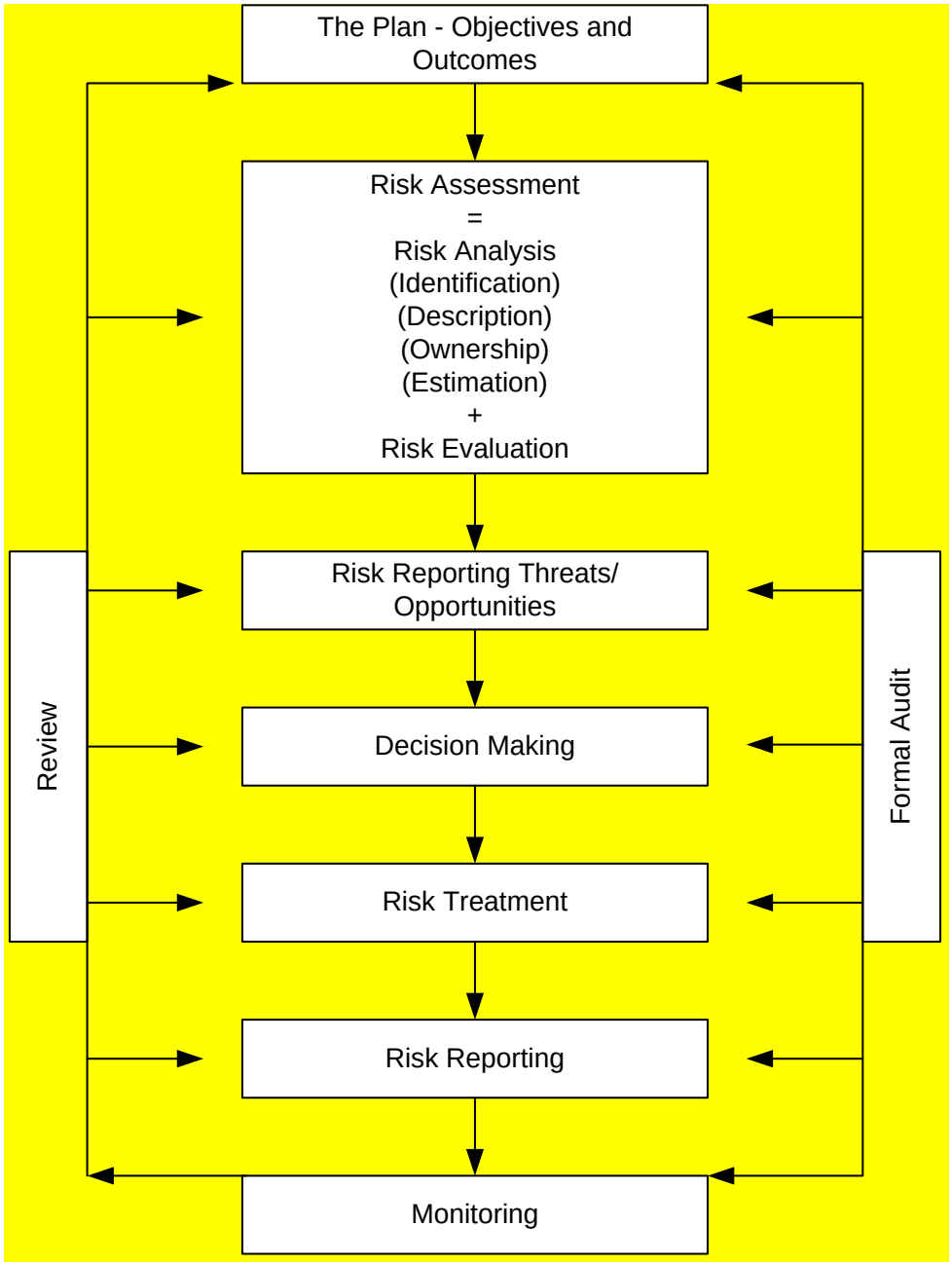


Figure 1: Risk Management Framework

2.4 Corporate risk management arrangements

2.4.1 Definition of corporate risk

Corporate risks are those, which if they occurred, would seriously affect the Authority's ability to carry out its core functions or deliver the objectives and outcomes ~~as~~ set out in The Plan. ~~its strategic planning documents.~~ This type of risk may be caused by a number of events or triggers which take place within the organisation or as a result of external influences. Potential sources of corporate risk are shown in the diagram in Appendix 1.

2.4.2 Identification

Within the West Midlands Fire Service, corporate risks may be identified in a variety of ways, for example by:

- The Fire and Rescue Authority and the Audit Committee as part of its strategic role in managing risk within the organisation;
- ~~Corporate Board~~ Strategic Enabling Team (SET), as part of their collective strategic leadership responsibility in reviewing The Plan, its objectives and outcomes. ~~through their involvement in Corporate Performance Review meeting which reviews corporate risk, as part of their individual and collective responsibility as Risk Owners or as part of the strategic decision making role through the inclusion of risk information within papers submitted for Board approval;~~ As part of this process corporate risks will be reviewed and where appropriate refreshed to ensure they remain aligned to corporate objectives and outcomes; or in supporting the CFO's decision making through the inclusion of risk information within papers submitted for SET consideration; as part of their individual responsibility as Risk Owners.
- Quarterly Performance Review (QPR), as part of its role in monitoring and managing strategic performance and level 2 Action Plans a corporate risk position statement is submitted and the effectiveness of corporate risk arrangements in supporting the delivery strategic outcomes and objectives is reviewed and monitored.
- As a result of any intelligence generated by organisational and operational intelligence pathways.
- As part of the work of the Organisational Assurance Team.
- Any group or member of the organisation, through the relevant Line Manager and Strategic Enabler.

In each case, it is the responsibility of the Risk Owner with the support of the corporate risk lead in the Strategic Hub ~~lead officer for corporate risk (SPIRiT)~~ to support the identification process and present the relevant information to SET ~~Corporate Board via the Corporate Performance Review meeting~~. This information will be presented in the form of a Corporate Risk Assurance Map which will include:

- A description of the risk to the organisation;
- Any links between the risk and organisational objectives; ~~and/or performance indicators~~;
- A summary of those events which may cause the risk to occur (Triggers);
- A summary of the likely impacts if the risk does occur;
- Details of any existing or proposed control measures designed to reduce the likelihood or impact associated with the risk;
- Details of the assurance provided for control measures designed to reduce the likelihood or impact associated with the risk; and
- An estimation of the level of risk. ~~and an indication of the Authority's appetite for that risk.~~
- An overall confidence opinion as to the quality of the risk control environment.
- ~~the Strategic Advisory Group (SAG), as part of its role in identifying and developing strategic objectives and managing level 2 Action Plans. Also the identification of opportunities and threats and as part of the Corporate Performance Review meetings which reviews corporate risk.~~

- ~~the Programme Support Office, as part of its monitoring and management of programme and project risk registers.~~
- ~~the Community Safety Team, through its development, monitoring and managing of risk register(s) associated with Operations partnerships~~
- ~~any group or member of the organisation, through the relevant Line Manager and Director.~~

2.4.3 Description

All corporate risks are described clearly so that the nature of the risk is understood for example, 'Unable to respond to (a certain anticipated event), resulting in (the unplanned or unwanted event occurring)'. Each risk is then considered against one or more of the following categories, in order to assist the subsequent estimation process (see paragraph 2.4.5):

- **People:** The ability of the Authority to provide sufficient numbers of skilled, competent, motivated and effective employees.
- **Financial**: the ability of the Authority to meet its financial commitments, such as internal budget constraints or to provide value for money.
- **Environmental**: the environmental consequences and issues of sustainability associated with pursuing the Authority's strategic aims and objectives.
- **Reputation**: the impact upon the reputation of the West Midlands Fire Service within the local, or wider, community and the need to meet the current or changing needs and/or expectations of customers.
- **Service Delivery**: the impact upon the Authority's ability to deliver its strategic objectives to respond to changes in demographic, residential or socio-economic trends.
- **Physical**: the impact upon the Authority's ability to maintain a safe working environment.
- **Legal and Litigation**: the impact of failing to comply with, or adequately enforce, national or European law.
- **Information Communication Technology and Systems**: the impact upon technology used within the Authority or upon which it is reliant.
- Or any other category considered appropriate to adequately assess a given risk.

2.4.4 Ownership

An essential requirement in the management of any risk is to make sure that the correct people are identified and that they take on responsibility for that risk. Specific roles in the management of Corporate risk are the:

- Risk Owner: the person with overall responsibility for monitoring the progress being made in managing a given risk. In relation to corporate risks this is a Strategic Enabler. ~~normally a Corporate Board member.~~
- Control Owner(s): those people responsible for implementing the agreed control measures to manage the risk and informing the Risk Owner of the effectiveness of those control measures. In relation to corporate risks this is normally a Strategic Enabler ~~Corporate Board member~~ or a Middle Manager ~~senior manager~~.

2.4.5 Estimation

Estimation should be completed by those people having a full understanding of the risk, the related control measures and the potential outcomes, in relation to corporate risk this is the risk owner.

The estimation of corporate risk combines the two elements of LIKELIHOOD and IMPACT, that is:

Risk estimation = likelihood x impact

The likelihood is a measure of the probability of a given risk occurring, using a scale of 1 (LOW) to 4 (HIGH). The impact is a measure of the severity or loss of opportunity should that risk occur, again using a scale of 1 (LOW) to 4 (HIGH).

The risk estimation is informed ~~The level of risk is assessed~~ by using the relevant descriptors of likelihood and impact, as detailed in Appendix 2, with the overall score being the highest value obtained.

The descriptors will be reviewed periodically as part of the review of the risk management strategy and presented to the Audit Committee for approval.

2.4.6 Evaluation

The purpose of risk management is not to eliminate all risk, but to reduce it to a level that is considered acceptable within an organisation, or to society.

Evaluation is undertaken to make informed decisions as to the significance of the risks to the Authority and to determine whether they will be accepted or treated, and what level of monitoring will be required.

As part of the evaluation process, a target score will be established for each risk by the relevant owner. This target score provides an indication of the Authority's risk appetite and acts as a guide for the allocation of time, effort and resources when managing a specific risk.

2.4.7 Reporting and Corporate Risk Assurance Mapping

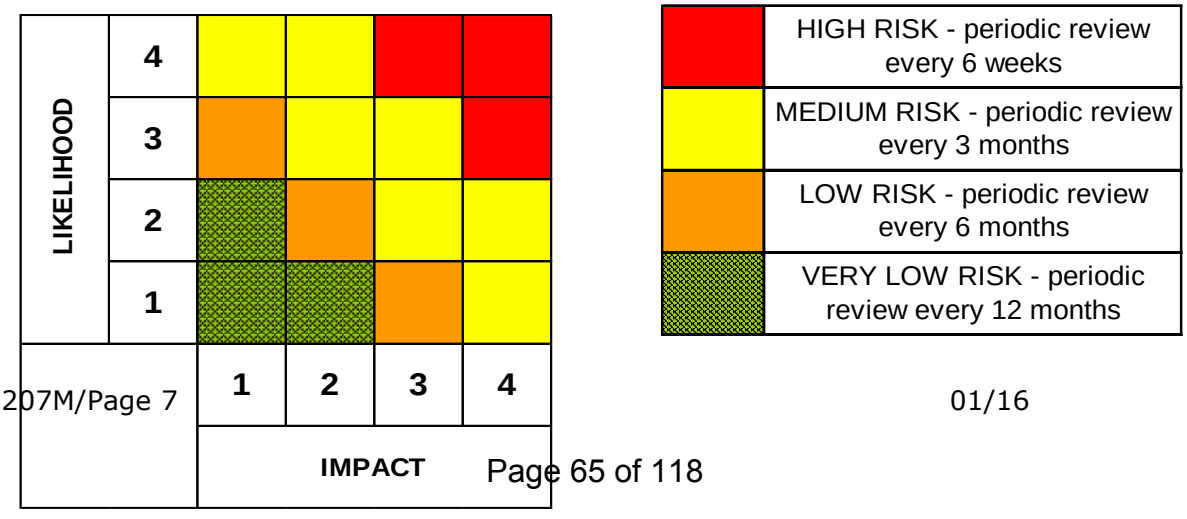
The Corporate Risk Assurance Map Summary is designed to provide an overview of the Service's corporate risks, Risk Owners, the risk rating ~~(likelihood x impact score, risk level)~~ and a direction in travel judgement based upon comparison with the previous quarterly review. ~~summary~~. ~~The Corporate Risk Assurance Map Summary is submitted on a quarterly basis to the Audit Committee following approval at the Corporate Performance Review meeting.~~

Each quarterly Corporate Risk Assurance Map Summary will be supported by a detailed Position Statement, designed to provide an update of the effectiveness of the control environment including confirmation of the overall risk rating, significant changes, amendments or additions to risk control measures and the identification of any assurances provided to risk controls. Both the summary and Position Statement will be reported to QPR.

Audit Committee will be presented with the summary and Position Statement twice yearly. Should there be any significant change to the corporate risk environment, Audit Committee will be informed of this at the next available Audit Committee meeting. In order to build and maintain Audit Committee Members capability and to ensure their continued engagement in corporate risk issues, timely and relevant reports on specific corporate risk topics will be presented by Officers to Audit Committee.

Both the summary and Position Statement will be available to the general public via the Committee Management Information System (CMIS). ~~This information is also published on the SPIRiT intranet site.~~

The Risk Owner will review corporate risks as set out on the Corporate Risk Assurance Map periodically. This will be undertaken in accordance with the following schedule:



The Corporate Risk Assurance Map sets out and details the triggers ~~or events~~ (those things that could cause the overall corporate risk to be realised), controls measures in place to reduce the likelihood or impact of risk realisation and Control Owner who is responsible for each control. Additional controls - that is controls being developed that are designed to strengthen the control environment to further reduce the likelihood and impact of risk realisation - are also detailed on the map along with a timeline for implementation of the additional control and Control Owner.

The outcome of the periodic review will inform the Position Statement that is submitted to ~~the Corporate Performance Review meeting~~ QPR and the Audit Committee. ~~on a quarterly basis along with the Corporate Risk Assurance Map Summary.~~

In order to provide confidence to Members and the CFO ~~and Corporate Board alike~~ as to the effectiveness of the control measures in place to manage corporate risks the Service operates a 'three lines of defence' assurance model.

This model is designed to encourage personal responsibility and requires Control Owners to periodically provide an assurance opinion as to the effectiveness of each control measure for which they are responsible. Assurance provided by Control Owners is known as the first line of defence.

The second line of defence seeks to provide a level of independent assurance, that is, that which is not provided by Control Owners. This may be given through various means such as the Organisational Assurance Team review near hits, organisational or operational Intelligence, accident investigations and recommendations from other reviews. ~~or as part of a sampling exercise conducted by the lead officer for corporate risk (SPIRiT) Manager. Peer reviews (Operational Assessment) reviews to ensure legal compliance (Health and Safety Executive for example) and those undertaken by accredited bodies (Investors in People for example) may also provide assurance at this level.~~

~~The~~ Internal Audit and External Audit function provide the third line of defence assurance. This provides an overall assurance to CFO ~~Corporate Board~~ and Fire Authority as to how effectively the Service manages its risks. The Internal Audit function has in place a three year Internal Audit strategy and annual audit plan which provides sufficient coverage of the Service's risk environment. Peer reviews (Operational Assessment) reviews to ensure legal compliance (Health and Safety Executive for example) and those undertaken by accredited bodies (Investors in People for example) may also provide assurance at this level.

All assurances given will be recorded on the Corporate Risk Assurance Map and will inform the Internal Audit strategy and Plan.

As part of the review process, the Risk Owner will provide an overall confidence opinion as to the strength of the control environment for each corporate risk for which they are responsible. This will be informed by the individual effectiveness opinion awarded to each control as part of the three lines of defence approach to assurance. Effectiveness and the confidence opinions are detailed on the Corporate Risk Assurance Map which is available electronically on a shared drive to all Risk and Control Owners.

~~It will be the responsibility of the lead officer for corporate risk (SPIRiT) to facilitate the above reporting and review process.~~

2.4.8 Treatment

Upon completion of the risk assessment process, it is important that risks identified are subject to a process of treatment. The purpose of this is to take appropriate action in order to minimise the likelihood of the risk occurring and/or reduce the severity of the consequences should it occur.

Most commonly, treatment involves the implementation of additional measures to control a risk before it occurs or to lessen the effects after it has occurred. In the case of corporate risk, this is the most likely action to be taken.

However, this is just one method of treatment; the following list provides a hierarchy of measures that may be implemented either in isolation or in combination.

- Termination: using an alternative approach that either involves lower levels of risk or no risk at all. This technique is not always an option.

- Treatment: the development, implementation and monitoring of measures designed to reduce the risk to an acceptable level. This may be achieved by introducing new policies or working practices. All such control measures must be monitored to ensure that they are effective and having a positive impact.
- Toleration: simply accepting the level of risk and proceeding without any additional action. This is not a control measure and should be discouraged as a course of action.
- Transfer: passing responsibility for the risk to a third party, such as a specialist contractor. Although an effective measure, it may incur some cost.
- Contingency (insurance): these are actions planned to come into force as and when a risk occurs. The most common risk management tool, insurance provides financial protection against the realisation of risk.

2.5 Other risk registers

As part of the portfolio approach to risk management, the Service should maintains risk registers at levels other than the corporate level. In accordance with its planning framework the risks associated with the delivery of all action plans, programmes and projects should be identified, ~~These registers are to be~~ reviewed, reported and monitored using in line with a clearly defined risk management process and should follow the principles set out in 2.3 and 2.4 above. Effective risk management will enable for the achievement of objectives, outputs and outcomes at these other levels and, in respect of those levels listed below, enables the Service to consider the level of control that exists in these other levels and whether there are any risks that require consideration in a corporate risk context.

2.5.1 Programme and project risk

Risk within the programme and project environment will be reported through stage reviews and highlight reporting processes to ~~Senior~~ Responsible Owners or Programme Management Board (or its equivalent) as appropriate. Responsible Owners ~~The Programme Manager (Programme Support Office)~~ will be responsible for ensuring that any independencies and risks associated with projects are identified, recorded, managed and reviewed. ~~periodically review all project risk registers to identify any interdependencies and where appropriate escalate to the programme risk register.~~ It is important that any risks associated with high level programmes or projects (those that carry significant risks, complexity or cost for example) are made known to ~~The Programme Manager will liaise with~~ the lead officer for corporate risk ~~(SPIRiT)~~ (Strategic Hub) to ensure that the potential impacts upon corporate risks, arising from the programme and project environment, can be determined.

2.5.2 Partnership risk

West Midlands Fire Service works in conjunction with a wide range of partners to enable for the delivery of services to the community. In order to ensure that every partnership entered into satisfies certain criteria, a partnership framework has been developed and is detailed in Standing Order 22/2.

As part of the framework, an assessment of risk will be carried out for each partnership at the initial proposal stage. All partnerships will continue to monitor and evaluate risks throughout the term of the partnership.

In respect of ~~Operations~~ Service Delivery partnerships, the ~~Head of Community Safety~~ the Strategic Enabler for Prevention will maintain a record of all risk assessments and this will form the partnership risk register for the Organisation. This register will be reviewed on a quarterly basis and risks assigned a high risk rating will be forwarded to the lead officer for corporate risk ~~(SPIRiT)~~ in Strategic Hub so that their impact upon corporate risk can be determined.

2.5.3 Action plans

The action planning template enables the identification, assessment and ongoing management of risk at all levels of planning. In respect of strategic level 2 plans, the Strategic Enabler ~~Advisory Group member~~ with designated responsibility for a particular level 2 action plan will be responsible for ensuring the completion and maintenance of the risk log information on the action planning template. Any risks given a 'high' risk rating

should be forwarded to the lead officer for corporate risk ~~(SPIRiT)~~ (Strategic Hub) so that their impact upon corporate risk can be determined.

2.6 Roles and responsibilities

Risk management is an integral part of every manager's role and impacts upon their day to day activity. It enables informed judgements to be made about the suitability and effectiveness of policy options and delivery methods. As such, it is a key element of both corporate and departmental planning, resourcing and service delivery.

However, there are certain roles within the organisation to which specific responsibilities are assigned in relation to Corporate Risk. These roles include:

- Fire Authority and Audit Committee: The Corporate Risk Assurance Map Summary will be reported six monthly ~~quarterly~~ to the Audit Committee and at least annually to the Fire Authority (via Audit Conmmittee minutes). In order to enable Members to understand the strategic risks faced by the organisation and to participate in their ownership through analysis and questioning and promoting a positive attitude towards the management of risk, timely and relevant reports on a range of risk topics will be presented to Audit Committee.
- ~~Corporate Board~~ SET: to show a clear commitment to the ownership of the risk management framework; agreeing and supporting the risk management strategy; identifying corporate risks and determining the effectiveness of associated control measures; demonstrating a willingness to accept risk in a managed way and within agreed tolerance levels and allocate resources accordingly.
- Risk owner: the person, ordinarily a member of SET ~~Corporate Board Member~~, with overall responsibility for monitoring the progress being made in managing a given corporate risk. This includes providing an overall confidence opinion as to the effectiveness of the control environment.
- Control owner(s): those people responsible for implementing the agreed control measures to manage the risk and informing the risk owner of the effectiveness of those control measures. This includes providing an assurance opinion as to the effectiveness of those controls for which they are responsible.
- ~~Strategic Advisory Group~~ QPR: As the strategic leads for the delivery of level 2 plans to identify, monitor risks and control measures (via the position statement) and where appropriate report on those risks to the lead officer for corporate risk ~~(SPIRiT~~) (Strategic Hub).
- ~~Programme Manager (Programme Support Office): monitor the risks associated with programmes and projects within their remit and where appropriate to report on those risks to the lead officer for corporate risk (SPIRiT).~~
- Head of Community Safety: to ensure that arrangements are in place to enable for the effective identification and monitoring of partnership risks and associated control measures of all Operations partnerships throughout the organisation in accordance with Standing Order 22/2.
- Lead officer for corporate risk ~~(SPIRiT):~~ (Strategic Hub): to assist in the implementation of all aspects of the risk management strategy.

2.7 Review and audit

The management of risk within the organisation and the effectiveness of the risk management strategy will be subject to an ongoing review process. Risk Management is a core component of the Organisation's internal audit plan and strategy and aspects of it are reviewed annually.

3. CROSS REFERENCES

The information contained in this Standing Order makes reference to information contained in:

Standing Order 1/2 Orders and Strategies

~~Standing Order 1/9 Project and Programme Management Process~~

Standing Order 1/31 Business Continuity

Standing Order 19/6 Risk Assessment

Standing Order 22/2 Partnership Working

Standing Order 22/6 Integrated Planning Process

Operational Guidance – Incident Command

4. KEY CONSULTEES

~~Corporate Board members~~ SET and Authority members.

5. EQUALITY IMPACT ASSESSMENT

In compiling this strategy an Initial Equality Impact Assessment has been completed. The assessment identified that the management of risk within the organisation will have a positive impact upon all identified groups by reducing the likelihood of negative threats and so increasing the likelihood of positive opportunities.

6. OWNERSHIP

~~This Standing Order was presented to Corporate Board on 4 December 2012, Audit Committee on 7 January 2013 and was approved by the Fire Authority on 18 February 2013.~~

This Standing Order was presented to SET on 4 December 2012, Audit Committee on 7 January 2013 and was approved by the Fire Authority on 18 February 2013. This Standing Order will be submitted for approval by the Audit Committee 6 June 2016.

7. RESPONSIBILITY AND REVIEW/AMENDMENT DETAILS

7.1 Responsible Corporate Board Member/Department

~~This Standing Order is the responsibility of the Director Technical and Operational Support.~~

Strategic Enabler, Strategic Hub

7.2 Created/fully reviewed/amended

~~It was created by the Corporate Risk Manager in November 2007 and subsequently amended and updated in February 2009, March 2010, December 2012 and February 2013.~~

Reviewed and amended in May 2016 by Strategic Hub and The Policy Team.

Sources of Corporate Risk

RISK MANAGEMENT STRATEGY
CORPORATE RISKS DESCRIPTORS

Rating	LIKELIHOOD	IMPACT People	IMPACT Financial	IMPACT Environmental Sustainability	IMPACT Reputation	IMPACT Service Delivery	IMPACT Physical Injury	IMPACT Legal/Litigation	IMPACT ICT/Systems
4	Very High >50% or Likely to occur within current financial year	Major adverse impact upon the ability to provide sufficient numbers of skilled, competent and motivated employees	Unplanned costs in excess of £1m	Major adverse impact on the environmental strategy of the organisation	Significant adverse publicity at national level	>25% of Corporate Objectives not delivered OR permanent impact on Service Delivery	Death of employee(s) or third party arising from Fire Service activity	Criminal prosecution of Authority Member/Executive Officer or Civil Litigation arising from death or other loss	Failure or significant disruption to mobilising and/or communications systems
3	High 25% to 50% or Likely to occur within two years	Significant adverse impact upon the ability to provide sufficient numbers of skilled, competent and motivated employees	Unplanned costs of £500k to £1m	Significant adverse impact on the environmental strategy of the organisation	Significant adverse publicity across region or within West Midlands area	11 to 24% of Corporate Objectives not delivered OR temporary impact on Service Delivery	Serious (RIDDOR) injuries to employee(s) or third party arising from Fire Service activity	Issue of Prohibition or Improvement Notice by an Enforcing Authority or Civil Litigation arising from serious injury or other loss	Failure or significant disruption to critical back office systems
2	Medium 10% to 24% or Likely to occur within five years	Minimal adverse impact upon the ability to provide sufficient numbers of skilled, competent and motivated employees	Unplanned costs of £150k to £499k	Minimal adverse impact on the environmental strategy of the organisation	Adverse publicity across West Midlands area	5 to 10% of Corporate Objectives not delivered or (no impact on Service Delivery)	Moderate injuries to third party as a result of Fire Service activity	Civil Litigation instigated by third party as a result of injury or other loss	Failure or disruption to non-critical corporate services
1	Low <10% or Unlikely to occur within next five years	No impact upon the ability to provide sufficient numbers of skilled, competent and motivated employees	Unplanned costs of less than £150k	No impact on the environmental strategy of the organisation	Adverse publicity confined to area within West Midlands	< 5% of Corporate Objectives not delivered	Minor injury to employee(s) not RIDDOR reportable	Civil Litigation instigated by employee as a result of minor injury or other loss	Failure or disruption to non critical local services

APPENDIX 2

CORPORATE RISK: AUDIT COMMITTEE BRIEFING

Trade Dispute & Action Short of Strike

Members will be aware that there is an ongoing review of the Shared Fire Control Function as determined by the Service Level Agreement when the Shared Fire Control was established. The outcomes of the review were presented to Shared Fire Control Governance Board (which has representation from both Staffordshire and West Midlands Authorities) in October 2015 with direction given to proceed with the planned changes.

The key aims of the review were to:

- Reduce personnel costs associated with Shared Fire Control (in the region of £430,000)
- Provide a more balanced level of supervision across the function

To support the achievement of the above a review of systems and processes continues to take place.

Trade Dispute

Despite the commitment of the Service to open and regular communication and negotiation with the Fire Brigades' Union (FBU) on this matter, the Shared Fire Control review was a constituent part of the ongoing wider trade dispute linked to staffing.

Following a ballot FBU members voted in favour of taking industrial action in the form of action short of strike (commonly known as ASOS). This included Fire Control staff and the specific ASOS planned to be utilised was a ban on personnel volunteering for overtime shifts.

Impact upon Service Delivery Model - The Risk

There is the potential that there will be a shortfall in numbers of personnel required to maintain an effective Fire Control function leading to delays in deploying our resources. This would directly affect our ability to meet attendance times and therefore have an impact on outcomes for the community; most notably survivability at our highest risk (Category 1) incidents.

ASOS was utilised on a night shift on 19th March 2016 for a period of 13 hours. This ASOS had no impact with staffing levels being high on that particular night shift.

How we are responding to the Risk

- The Service continues to maintain its commitment to communication and negotiation with representative bodies. There are regular meetings with the FBU and the Service with positive progress being made to reach a negotiated agreement.

- A revised offer taking on board feedback from staff and the FBU has been produced on 19th May 2016 and is currently being consulted upon through FBU branch meetings.

- The Service has in place effective day to day workforce planning arrangements to identify and manage potential shortfalls in staffing. In the event of ASOS being used we would still be able to maintain a Fire Control function with reduced numbers on a short term basis.

- Only 35%of FBU members voted for this course of action. This is a minority and means that 65% of eligible staff have either not felt they can support Industrial Action or have not had the opportunity to register their view.

- Business Continuity arrangements have been reviewed for suitability and we have retrained some ex-members of Fire Control and agreed flexibility from other members of Fire Control to cover any shortfalls.

Impacts upon Corporate Risks

Industrial action and the risk controls in place to prevent (likelihood) and mitigate against the impacts should it occur within Fire Control are recorded, monitored and managed against a number of our Corporate Risks, namely:-

1. The Fire Authority would be unable to maintain the positive engagement of its employees, resulting in an inability to deliver its key priorities and objectives.

5. The Fire Authority would be unable to deliver the core objectives of preventing, protecting and responding effectively as a result of extensive disruption to normal working methods.

6. The Fire Authority would be unable to ensure that operational incidents are dealt with safely and effectively using appropriate levels of resources and personnel.

11. The Fire Authority would be unable to maintain its command and control function, resulting in an inability to receive process and respond to emergency calls effectively

WEST MIDLANDS FIRE AND RESCUE AUTHORITY

AUDIT COMMITTEE

6 JUNE 2016

1. ANNUAL INTERNAL AUDIT REPORT – 2015/16

Report of the Audit Services Manager.

RECOMMENDED

THAT the Annual Internal Audit report for 2015/16 be approved.

2. PURPOSE OF REPORT.

This report is submitted for member comment and approval.

3. BACKGROUND

3.1 The attached report details the work of the internal audit service undertaken in 2015/16. It provides an opinion on the adequacy and effectiveness of the Authority's governance, risk management and internal control processes.

3.2 The contents of the report also provide one element of the evidence that is required to underpin the Authority's Governance Statement.

3.3 It summarises the audit work undertaken during the year in a tabular format, this includes:

- the areas subject to review during the year (Auditable Area)
- the level of risk to the Authority assigned to each auditable area (high, medium or low)
- the number of recommendations made as a result of each audit review
- details of any other work undertaken outside of the original plan

Finally it provides a summary of the key control issues that arose during the year.

4. EQUALITY IMPACT ASSESSMENT

In preparing this report an initial Equality Impact Assessment is not required and has not been carried out. The matters contained in this report will not lead to and/or do not relate to a policy change.

5. LEGAL IMPLICATIONS

The Accounts and Audit Regulations Act states that a relevant body must "maintain an adequate and effective system of internal audit of its accounting records and of its system of internal control in accordance with the proper internal audit practices".

6. FINANCIAL IMPLICATIONS

There are no direct financial implications arising from this report.

7. BACKGROUND PAPERS

Annual Internal Audit Report 2015/16.

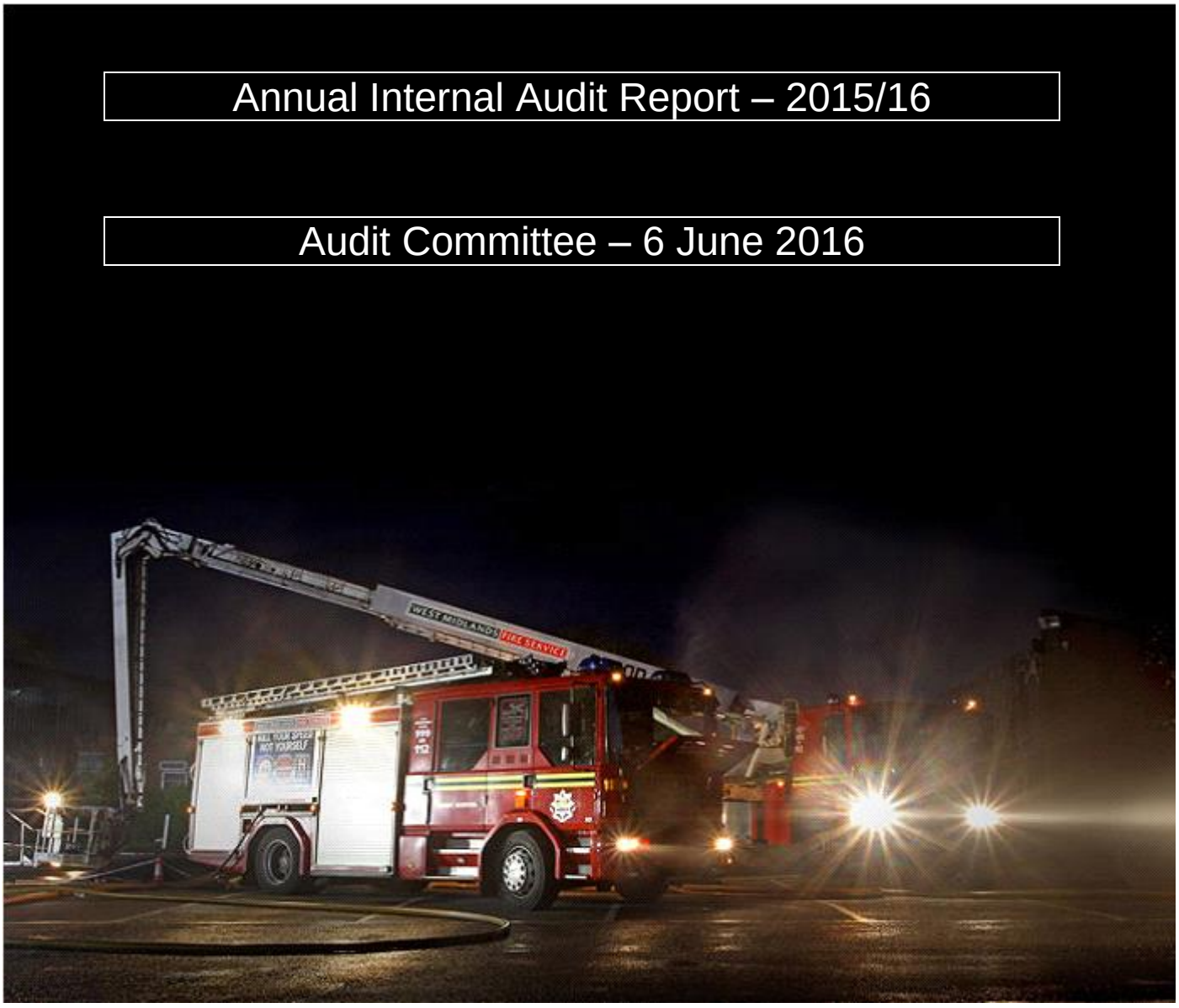
Peter Farrow
Audit Services Manager, Sandwell MBC

Ref. AU/AC/2016/June/12405169

WEST MIDLANDS FIRE SERVICE

Annual Internal Audit Report – 2015/16

Audit Committee – 6 June 2016



1 Introduction

1.1 Our internal audit work for the period from 1 April 2015 to 31 March 2016 was carried out in accordance with the approved Internal Audit Plan. The plan was constructed in such a way as to allow us to make a statement on the adequacy and effectiveness of the Authority's governance, risk management and control processes.

In this way our annual report provides one element of the evidence that underpins the Governance Statement the Authority is required to make within its annual financial statements. This is only one aspect of the assurances available to the Authority as to the adequacy of governance, risk management and control processes. Other sources of assurance on which the Authority may rely could include:

- The work of the External Auditors (currently Grant Thornton)
- The result of any quality accreditation
- The outcome of visits by HMRC
- Other pieces of consultancy or third party work designed to alert the Authority to areas of improvement
- Other external review agencies

1.2 The definition of internal audit, as described in the Public Sector Internal Audit Standards, is set out below:

"Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes."

Overall Assurance

1.3 As the providers of internal audit, we are required to provide the Fire Authority with an opinion on the adequacy and effectiveness of the governance, risk management and control processes. In giving our opinion it should be noted that assurance can never be absolute. The most that internal audit can provide is reasonable assurance that there are no major weaknesses in the Authority's governance, risk management and control processes. In assessing the level of assurance to be given, we have taken into account:

- All audits undertaken for the year ended 31 March 2016;
- Any follow-up action taken in respect of audits from previous periods;
- Any significant or fundamental recommendations not accepted by management and the consequent risks;
- Any limitations which may have been placed on the scope of internal audit; and
- The extent to which any resource constraints may impinge on the ability to meet the full audit needs of the Authority.

2 Internal Audit Opinion

2.1 We have conducted our audits in accordance with the Public Sector Internal Audit Standards. Within the context of the parameters set out in paragraph 1.3 above, our opinion is as follows:

2.2 Based on the work undertaken during the year and the implementation by management of the recommendations made, Internal Audit can provide ***reasonable assurance** that the Fire Authority has an adequate and effective framework of governance, risk management and control.

***We are pleased to report that this is an unqualified opinion and the highest level of assurance available to Audit Services. As stated in paragraph 1.3 “In giving our opinion it should be noted that assurance can never be absolute. The most that internal audit can provide is reasonable assurance that there are no major weaknesses in the Authority’s governance, risk management and control processes”.

Factors Influencing the Opinion and Issues Relevant to the Statement on Internal Control

2.3 In reaching this opinion, the following factors were taken into particular consideration:

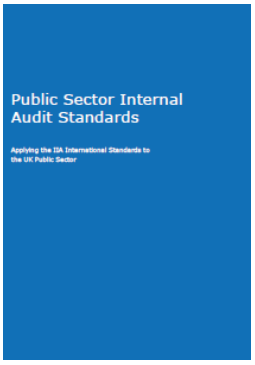
- The need for management to plan appropriate and timely action to implement both our and the External Auditor’s recommendations.
- Key areas of significance, identified as a result of our audit work performed in year are detailed in the Appendix to this report.

2.4 The overall opinion can be used by the Authority in the preparation of the Governance Statement.

2.5 Internal audit activity is organisationally independent and further details behind the framework within which internal audit operates, can be found in the internal audit charter.

3 Performance of the Audit Service

Compliance with the Public Sector Internal Audit Standards



During the year we complied with the revised Public Sector Internal Audit Standards which specify rules of conduct for objectivity, due professional care and confidentiality.

Customer Satisfaction

Customer satisfaction questionnaires are issued for all audits. From the responses returned, the average scores were as follows:

Question	2015/16
Usefulness of audit	4.0
Value of recommendations	4.0
Usefulness of initial discussions	4.0
Fulfilment of scope & objectives	4.7
Clarity of report	5.0
Accuracy of findings	5.0
Presentation of Report	5.0
Time span of audit	4.0
Timeliness of audit report	4.0
Consultation on findings/recommendations	4.7
Helpfulness of auditors	5.0
Overall Satisfaction with Audit Services	**4.5**

Scores range between 1 = Poor and 5 = very good. We have a target of achieving on average a score of **4 = good.**

Quality Assurance and Improvement Programme
Sandwell Audit Services have a Quality Assurance and Improvement Programme. During the year, the internal audit activity has followed this programme and there have been no significant areas of non-conformance or deviations from the standards as set out in the Public Sector Internal Audit Standards.

Staff are recruited, trained and provided with opportunities for continuing professional development. Staff are also supported in order to undertake relevant professional qualifications. All staff are subject to a formal staff appraisal process, which leads to an identification of training needs. In this way, we ensure that staff are suitably skilled to deliver the internal audit service. This includes the delivery of specialist skills which are provided by staff within the service with the relevant knowledge, skills and experience.

Advice and assistance
Finally, throughout the year we provide ongoing advice and assistance to all areas of the Fire Authority on internal control and related issues, including on the development of an assurance framework.

4 Summary of Work Completed to inform the 2015/16 Internal Audit Opinion

A detailed written report and action plan is prepared and issued for every internal audit review. The responsible officer will be asked to respond to the report by completing and returning the action plan. This response must show what actions have been taken or are planned in relation to each recommendation. If the recommendation is not accepted, this must also be stated. Audit Services are responsible for assessing whether the managers response is adequate.

Where appropriate each report we issue during the year is given an overall opinion based on the following criteria:

	Level	System Adequacy	Control Application
(positive opinions)	Substantial Assurance	Robust framework of controls ensures objectives are likely to be achieved.	Controls are applied continuously or with minor lapses.
	Satisfactory Assurance	Sufficient framework of key controls for objectives to be achieved, but control framework could be stronger.	Controls are applied, but with some lapses.
(negative opinion)	Limited Assurance	Risk of objectives not being achieved due to the absence of key internal controls.	Significant breakdown in the application of controls.

This is based upon the number and type of recommendations we make in each report. Each recommendation is categorised in line with the following:

Fundamental	Action is imperative to ensure that the objectives for the area under review are met.
Significant	Requires action to avoid exposure to significant risks in achieving the objectives for the area under review.
Merits attention	Action advised to enhance control or improve operational efficiency.

During the year we made the following number of recommendations:

Fundamental	0
Significant	4***
Merits attention	4
Total	**8**

The following appendices/tables below list of all the reports issued by internal audit during 2015/16, alongside their original Assessment of Assurance Need (AAN) risk score, the number and type of recommendations made, whether those recommendations have been accepted and an overall level of assurance for each review.

Key	
***	Recommendations made by External Auditors and followed up by Internal Audit.

Summary of Internal Audit Work Completed for the 2015/16 Internal Audit Opinion

Auditable Area	ANA Rating	Recommendations					Level of Assurance
		Fundamental	Significant	Merits attention	Total	Number accepted	
Pension Certification	High	-	-	-	-	-	-
Budgetary Control	KFS	-	-	-	-	-	Substantial
Procurement	Medium	-	-	-	-	-	Substantial
Accounts Receivable	KFS	-	-	-	-	-	Substantial
Fixed Asset Accounting/Asset Planning	KFS	-	-	-	-	-	Substantial
Accounts Payable	KFS	-	-	-	-	-	Substantial
Risk Management	High	-	-	-	-	-	Substantial
Governance	High	-	-	1	1	*	Substantial
Performance Management	Medium	**	**	**	**	**	**
Workforce Planning	Medium	**	**	**	**	**	**
Business Continuity	Medium	-	-	2	2	*	Substantial
IT	High	-	4***	-	4	4	-
Payroll	KFS	-	-	1	1	1	Substantial
Total		**-**	**4**	**4**	**8**	**5**	

Key	
KFS	Key Financial System (reviewed in line with External Audit requirements). Generally this is also a high risk review.
*	Action plan still under discussion in order to finalise the response.
**	At the time of the preparation of this report, our review of this area was underway and nearing completion. No key issues had been identified during the review that would impact upon our overall audit opinion.
***	Recommendations made by External Auditors and followed up by Internal Audit.

Key issues arising during the year

The following is a brief overview of the key issues identified during the year.

Local Government Pension Scheme Certification
An audit was undertaken to assist with the provision of assurance on the accuracy of the 2014/15 return to the Local Government Pension Scheme. All tests proved satisfactory.

Budgetary Control
A review of the budgetary control system was undertaken to ensure the Fire Service had established its budget and was managing it appropriately. Our review covered controls over monitoring, reporting, changes to budgets and the process to link budgets to medium and long term plans.

Procurement
A review of the procurement process was undertaken to provide assurance over the control of non-contract spend within the Fire Authority. It was established that:

- There was a clear strategy in place which enabled contracts to be procured in accordance with contract and procedure rules and on a timely basis.
- The sections within the Fire Authority were utilising the contracts in place.

Non-contract spend was well controlled.

Accounts Receivable
A review of the accounts receivable system was undertaken to ensure that an effective system was in place for raising invoices and managing debtors. This included the integrity and reliability of charging information recorded in the accounts, the collection of payments and the process to monitor and report the debtor position.

Fixed Asset Accounting/Asset Planning
An audit of fixed asset accounting was undertaken in respect of planned capital expenditure. The review was undertaken to provide assurance that an appropriate process was in place to maintain details of fixed assets and to record them correctly in the accounts.

Accounts Payable
A review of the accounts payable system was undertaken to ensure that adequate key controls were in place. Our review focused on the controls designed to prevent, overpayments, fraud and incorrect accounting.

Risk Management
An audit of the risk management processes was undertaken. Our review focused on providing assurance that the mitigating controls for risk 1 – “The Fire Authority would be unable to maintain the positive engagement of its employees, resulting in an inability to deliver its key priorities and objectives”, were being effectively operated and monitored. The review concluded that the risk was being effectively managed.

Governance
The review was based on the principles of the CIPFA/Solace document “Delivering Good Governance in Local Government: Framework” and focused on the

demonstration of the values of good governance through upholding high standards of conduct and behaviour and the taking of informed and transparent decisions which are subject to effective scrutiny and management of risk. The review focused on two of the core principles:

- Promoting values for the authority and demonstrating the values of good governance through upholding high standards of conduct and behaviour.
- Taking informed and transparent decisions which are subject to effective scrutiny and managing risk.

Only one issue was identified, noting that members of the Audit Committee will be re-visiting their self-assessment of good practice and effectiveness exercise early in the new year.

Performance Management
A review of performance management was undertaken to provide assurance that the systems in operation were effective in supporting the authority in achieving its priorities. Specifically that appropriate targets were set, performance was accurately calculated, reported, monitored and challenged. At the time of reporting, this review was being finalised, but there did not appear to any issues of significance.

Workforce Planning
A review of the workforce planning processes was undertaken to provide assurance on how well they were embedded within the authority. Included was a review of the plan itself and whether it reflected the priorities of the authority, had been appropriately compiled, approved, reviewed and monitored. At the time of reporting, this review was being finalised, but there did not appear to any issues of significance.

Business Continuity
A review was undertaken to provide assurance that appropriate arrangements were in place to enable services to continue to be delivered in the event of an incident occurring and that an appropriately skilled and resourced emergency planning and continuity function was being maintained and the requirements of the Civil Contingencies Act 2004 were complied with. The review concluded that an effective business continuity process was in operation. The only issues to be addressed related to evidencing the completion of the annual business impact assessment for each business continuity plan and to record when incident training had been undertaken.

IT
The external auditors for the Authority, had as part of their work for 2014/15, identified some issues and made recommendations relating to the IT function, specifically:

- Weak password access controls for the Oracle EBS system.
- No documented change management policy for IT system changes.
- Excessive number of domain administrators.
- The IT security policy had not been formally reviewed or updated since its establishment in September 2010.

A review was undertaken to identify whether these matters had subsequently been addressed. It was established that action had been taken to resolve these issues.

Payroll
A review of the payroll process was undertaken to ensure that the Fire Service had appropriate controls in place to mitigate the risk of fraud and error in the calculation, recording and payment of the payroll via BACS.

Follow Up
A review of actions taken in response to recommendations from the 2014/15 audits was completed. All recommendations had been implemented.

Other areas of assistance provided

Audit Committee Annual Report
Assistance was provided in the preparation of the Annual Report of the Chair, on the work of the Audit Committee.

Counter Fraud
We continued to lead on the Cabinet Office's National Fraud Initiative and their other associated fraud related activity (such as the Annual Fraud Survey), on behalf of the Authority and to provide the main point of contact for any investigations into potential fraudulent activity.

WEST MIDLANDS FIRE AND RESCUE AUTHORITY

AUDIT COMMITTEE

6 JUNE 2016

1. AUDIT COMMITTEE UPDATE FOR WEST MIDLANDS FIRE AND RESCUE AUTHORITY

Report of the Chief Fire Officer

RECOMMENDED

THAT the Committee note the content of the Audit Committee Update attached as an Appendix.

2. PURPOSE OF REPORT

The update is provided to keep Audit Committee Members informed of the progress of the external auditor (Grant Thornton UK LLP) in delivering their responsibilities.

3. BACKGROUND

3.1 In order to ensure that Audit Committee Members continue to remain informed on audit matters, the external auditor has provided an Audit Committee Update report. It is the intention of the external auditor to provide an update at all Audit Committee meetings.

3.2 The update provides the Audit Committee with a report on Grant Thornton's progress in delivering their responsibilities and also includes:-

- a summary of emerging national issues and developments that may be relevant to West Midlands Fire and Rescue Authority; and

- a number of challenge questions in respect of these emerging issues which the Committee may wish to consider.

3.3 Representatives from Grant Thornton will be in attendance at the meeting to discuss the reports with Members.

4. **EQUALITY IMPACT ASSESSMENT**

In preparing this report an initial Equality Impact Assessment is not required and has not been carried out. The matters contained in this report will not lead to a policy change.

5. **LEGAL IMPLICATIONS**

The course of action recommended in this report does not raise issues which should be drawn to the attention of the Authority's Monitoring Officer.

6. **FINANCIAL IMPLICATIONS**

There are no direct financial implications arising from this report.

BACKGROUND PAPERS

None

The contact officer for this report is Deputy Chief Fire Officer, Philip Hales, Telephone Number – 0121 380 6907.

PHIL LOACH
CHIEF FIRE OFFICER

Audit Committee Update for West Midlands Fire & Rescue Authority

Progress Report and Update Year ended 31 March 2016

June 2016

James Cook
Director
T 0121 232 5343
E james.a.cook@uk.gt.com

Emily Mayne
Manager
T 0121 232 5309
E emily.j.mayne@uk.gt.com

James McLarnon
Assistant Manager
T 0121 232 5219
E james.a.mclarnon@uk.gt.com

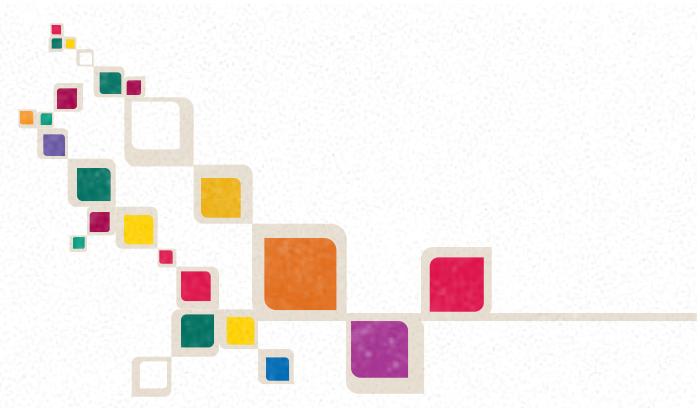
Introduction

This paper provides the Audit Committee with a report on progress in delivering our responsibilities as your external auditors.

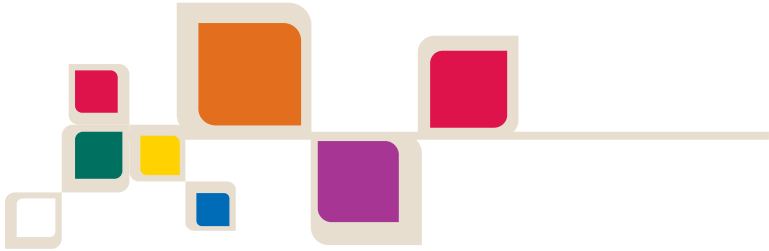
Members of the Audit Committee can find further useful material on our website www.grant-thornton.co.uk, where we have a section dedicated to our work in the public sector. Here you can download copies of our publications:

- Mental health collaboration: 'Joining up the dots, not picking up the pieces' (April 2016)
  http://www.grantthornton.co.uk/en/insights/partnership-working-in-mental-health/
- Better Together: Building a successful joint venture company (April 2016)
  http://www.grantthornton.co.uk/en/insights/building-a-successful-joint-venture-company/

If you would like further information on any items in this briefing, or would like to register with Grant Thornton to receive regular email updates on issues that are of interest to you, please contact either your Engagement Lead or Engagement Manager.



Progress to date



2015/16 work	Planned Date	Complete?	Comments
Fee Letter We are required to issue a 'Planned fee letter for 2015/16' by the end of April 2015.	April 2015	Yes	The 2015/16 fee letter was issued in April 2015
Accounts Audit Plan We are required to issue a detailed accounts audit plan to the Fire Authority setting out our proposed approach in order to give an opinion on the Fire Authority's 2015/16 financial statements.	March 2016	Yes	We continue to assess the risks facing your Authority and meet with Senior Officers to ensure that these risks are fully understood and our audit work is appropriate. If there are any changes to our plan between our initial risk assessment and the delivery of our opinion we will discuss this with the Strategic Enabler for Finance and Resources before presenting to the Audit Committee.
Interim accounts audit Our interim fieldwork visits include: • updating our review of the Fire Authority's control environment • updating our understanding of financial systems • review of Internal Audit reports on core financial systems • early work on emerging accounting issues • early substantive testing • proposed Value for Money conclusion.	January – March 2016	Yes	We will: • engage with the finance team to streamline and improve the audit approach for 2015/16 where possible • Discuss any technical issues early, including the impact from the pension commutation guidance • Undertake as much early testing as possible. We will continue to work closely with Internal Audit in relation to risk, work on the financial statements and fraud.
Final accounts audit Including: • audit of the 2015/16 financial statements • proposed opinion on the Fire Authority's accounts • proposed Value for Money conclusion.	June – September 2016	Not started	We will undertake work on your draft financial statements to provide an opinion by the statutory deadline. We are planning to complete our audit by 31st August. as part of the transition to the earlier closedown and audit cycle from 2017.

Progress to date

2015/16 work	Planned Date	Complete?	Comments
Value for Money (VfM) conclusion The scope of our work to inform the 2015/16 VfM Conclusion requires conclusions on whether: *"In all significant respects, the audited body had proper arrangements to ensure it took properly informed decisions and deployed resources to achieve planned and sustainable outcomes for taxpayers and local people".* This change of guidance was issued by the National Audit Office in November 2015. The Code requires auditors to satisfy themselves that; "the Authority has made proper arrangements for securing economy, efficiency and effectiveness in its use of resources". The three sub criteria for assessment to be able to give a conclusion overall are: • Informed decision making • Sustainable resource deployment • Working with partners and other third parties	March – July 2016	In progress	We have considered the potential significant risks for our VfM conclusion and identified the following issues. • Financial resilience • Working with partners and other third parties Our work on the VfM Conclusion will include attending meeting with key Senior Officers and key document reviews. We are aiming to deliver this work ahead of the national timescales as a move towards the faster close from 2017.
Annual Audit Letter We will summarise all the work completed as part of our 2015/16 audit within one letter which will be issued after the opinion.	October 2016	Not started	
Engagement with the Fire Authority since the last Audit Committee meeting	On-going	On-going	• Meetings with key Senior Officers to discuss progress with the significant risks facing the Fire Authority and VfM Conclusion risk areas • Distribution of Grant Thornton publications as appropriate to the Fire Sector

Fire Sector Accounting and other issues

Health and Safety in the Fire and Rescue Service

The HSE does not undertake a proactive programme of inspections across the FRS sector due to the good historical safety record and proactive culture with the FRS sector. To ensure these high standards remain the HSE works closely with CFOA to understand developments and support continuous improvement. The good working relationship between CFOA and HSE fire policy officers means firefighter safety in the operational environment is being discussed at a high level and work to implement change and best practice is being carried out.

Work between the Chief Fire Officers Association (CFOA) and the national Health and Safety Executive means the importance of firefighter safety remains at the forefront of Fire and Rescue Services agenda. *'Health and Safety in the Fire and Rescue Service – Embedding Lessons Learned'* , is a jointly produced document by the Chief Fire and Rescue Advisors in England & Wales, HM Fire Service Inspectorate in Scotland and the Health and Safety Executive but with full support and involvement of CFOA. Please see the document produced as a result of the work. http://www.cfoa.org.uk/20752

The document is seen as a simple and cost effective way to keep the health and safety of firefighting staff on the agenda. It touches upon a number of subjects, with particular emphasis as a reminder to all UK FRSs that lessons learned must be recognised at the initial stages of planning and development within organisations. Roy Wilsher, CFOA Director of Operations said: 'This is a very significant piece of work as it recognises the considerable progress that Fire and Rescue Services have made in their understanding of health and safety and balancing risk against benefit. I am pleased to be able to say that this has been achieved through the excellent working relationship between CFOA, the HSE, CFRA in England and Wales, HM Fire Service Inspectorate in Scotland and other partner agencies.'

Challenge questions

Are members aware of this publication and are officers responding appropriately to the learning in this document?

Grant Thornton Publications

Joining up the dots, not picking up the pieces

Partnership working in mental health

Grant Thornton reports

Challenge question:

Is the trust familiar with this report?

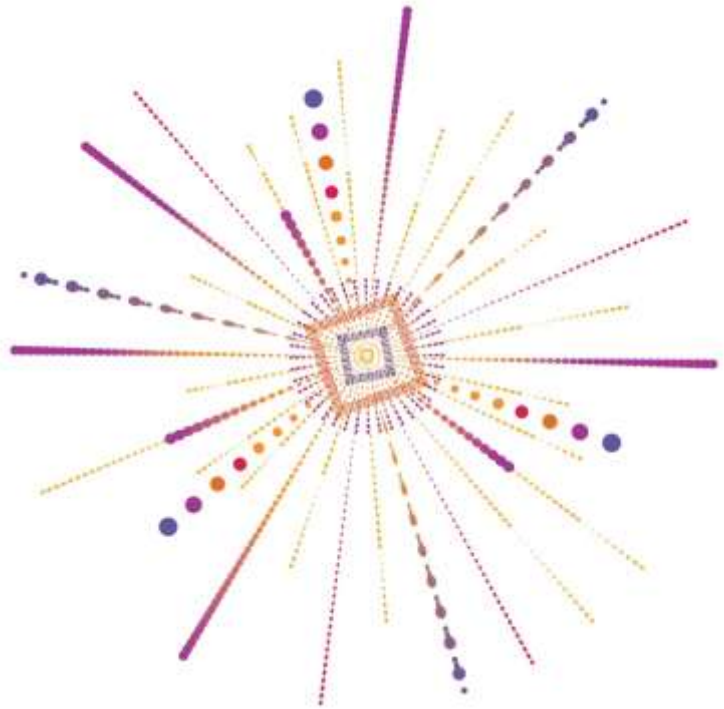
Summary report of our mental health collaboration summit

Mental ill health costs the economy over £100 million each year and affects one in four people. However, responding to issues related to an underlying mental illness does not solely sit within the remit of health professionals. With many parts of the public sector needing to respond, and each facing significant financial pressures, collaboration around this issue is essential to provide high quality care and make savings to the wider public purse.

This paper draws together examples of successful collaboration between public services and feedback from a Midlands round table discussion – where the West Midlands Combined Authority has set up a mental health commission – to look at how different services have overcome some of the traditional barriers and demarcation lines between organisations.

The key messages are:

- The unpredictable nature of mental health symptoms can mean that the first point of contact is via emergency services, with ambulance, fire and rescue or police officers being present. The cost of services not being available at the right place at the right time can be huge, in terms of the personal suffering of individuals and costs to the wider system
- Often relatively modest amounts of money targeted at specific initiatives such as street triage or community cafes can make a huge difference in improving the availability of important services
- An impact can be made without the need for expensive structural change. Most importantly, it requires a genuine approach to collaboration and a culture of putting the patient first
- Investing in collaborative initiatives focussing on the needs of mental health patients were undoubtedly resulting in savings elsewhere to the public purse. Examples include:
    - 92% reduction in detentions under section 136 of the Mental Health Act in Cheshire and Wirral; 50% reduction in Birmingham and Solihull; 39% in Nottinghamshire; 30% in Kent
    - 647 A&E attendances avoided by one street triage team in one year in Birmingham and Solihull
    - 80% remission in psychosis through early intervention in Derbyshire
    - 25% of unemployed users of the café run by the Manchester Mind Young Adults Services and Projects team have gone on to find employment.



Better together
Building a successful joint venture company

Grant Thornton market insight

Local government is continuing to innovate as it looks for ways to protect front line services. The changes are picking up pace as more local government bodies introduce alternative delivery models to generate additional income and savings. While these new models are not a solution by themselves, they do add to the wider solutions being explored by local government such as devolution, collaboration and integration.

Joint Ventures (JVs) have been in use for many years in local government and remain a common means of delivering services differently. This report draws on our research across a range of JVs to provide inspiring ideas from those that have been a success and the lessons learnt from those that have encountered challenges. The report also provides advice and information about the key areas to consider when deciding to set up a JV, setting it up and making it successful.

Key findings from the report:

- **JVs continue to be a viable option** – Where they have been successful they have supported councils to improve service delivery, reduce costs, bring investment and expertise and generate income
- **There is reason to be cautious** – Our research found a number of JVs between public and private bodies had mixed success in achieving outcomes for councils
- **There is a new breed of JVs between public sector bodies** – These JVs can be more successful at working and staying together. There are an increasing number being set up between councils and wholly-owned commercial subsidiaries that can provide both the commercialism required and the understanding of the public sector culture

grantthornton.co.uk

GRT102468

Agenda Item No. 9

WEST MIDLANDS FIRE AND RESCUE AUTHORITY

AUDIT COMMITTEE

6 JUNE 2016

1. ANNUAL REPORT OF THE AUDIT COMMITTEE 2015/16

Report of the Chair of the Audit Committee.

RECOMMENDED

That the Committee gives consideration to the content and format of its Annual Report 2015/16 for submission to the next full meeting of the Authority.

2. PURPOSE OF REPORT

This report is submitted to members to seek approval to the Annual Report of the Audit Committee 2015/2016.

3. BACKGROUND

3.1 In order for the Authority to be fully effective in comprehending and assessing the control environment within which West Midlands Fire Service operates, the Audit Committee present an annual report of its activities to the Authority.

3.2 A draft Annual Report for 2015/16 has been prepared by the Chair of the Audit Committee and is attached for comments by the Committee in preparation for submission of the report to the next Authority meeting.

4. EQUALITY IMPACT ASSESSMENT

In preparing this report an initial Equality Impact Assessment is not required and has not been carried out because the matters contained in this report do not relate to a policy change.

5. LEGAL IMPLICATIONS

The Authority has a duty under the Local Government Act 1999 to make arrangements to secure continuous improvement in the way in which its functions are exercised, having regard to a combination of economy, efficiency and effectiveness.

6. FINANCIAL IMPLICATIONS

The Accounts and Audit Regulations Act states that a relevant body must “maintain an adequate and effective system of internal audit of its accounting records and of its system of internal control in accordance with the proper internal audit practices”.

BACKGROUND PAPERS

Annual Internal Audit Report 2015/16.

Tersaim Singh
Chair of the Audit Committee

Ref. AU/AC/92405164

APPENDIX 1

WEST MIDLANDS FIRE SERVICE

Annual Report of the Audit Committee 2015/16

Ref. AU/AC/92405164

1. Background

The Audit Committee was established by the Fire Authority in January 2008. Its purpose is to provide:

- independent assurance on the adequacy of the risk management framework and the associated control environment,
- independent scrutiny of the authority's financial and non-financial performance to the extent that it affects the authority's exposure to risk and weakens the control environment, and to
- oversee the financial reporting process.

The key benefits of the Committee can be seen as:

- Increasing public confidence in the objectivity and fairness of financial and other reporting.
- Reinforcing the importance and independence of internal and external audit and similar review processes.
- Providing additional assurance through a process of independent review.
- Raising awareness of the need for internal control and the implementation of audit recommendations.

The Terms of Reference for the Committee can be found at Appendix A of this report.

Audit Committee Members Knowledge and Skills Framework
Each member of the Committee is currently completing a knowledge and skills framework questionnaire, giving them the opportunity to record details of their relevant experience and knowledge, and to identify areas where they felt they would benefit from additional training. Once these have been completed, the results will be summarised and reported back to the Committee.

2. Meetings

During 2015/16 the Committee met on the following dates:

- 15 June 2015
- 7 September 2015
- 9 November 2015
- 18 January 2016
- 11 April 2016

3. Committee members and attendance record

	15/06/15	7/09/15	9/11/15	18/01/16	11/04/16
Councillor T Singh	√	√	√	√	√
Councillor Aston	X	X	√	√	√
Councillor Mottram	√				
Councillor Quinnen	√	√	√	X	√
Councillor P Singh		√	√	√	X
Councillor Miks		√	X	√	√
Councillor Sealey		√	X	√	√
Mr M Ager	√	√	√	√	√

4. The Committee's business

During the year the Committee conducted the following business:

Governance Statement - 2014/15	CIPFA Audit Committee Updates
Corporate Risk – Regular Updates	Updates on Topical, Legal and Regulatory Issues
Audit Committee Annual Report – 2014/15	Treasury Management Annual Report – 2014/15 (and Mid-Year Review)
Audit Committee – Terms of Reference Review	Monitoring Policies on Raising Concerns at Work – Whistleblowing Standing Order and Regulation of Investigatory Powers Act
Audit Committee – Self Assessment of Good Practice (continuing)	Value for Money for the Authority
Audit Committee Work Programme	
External Audit Work Programme and Scale of Fees	Internal Audit Annual Report - 2014/15
External Audit Plan	Internal Audit Progress Reports
External Audit – Annual Audit Letter 2014/15	Internal Audit Charter – Annual Review
External Audit – Audit Committee Updates	Internal Audit Plan – 2016/17
External Audit – Communication with the Audit Committee	Review of the Effectiveness of Internal Audit
Update from the Pensions Board – Firefighters Pension Scheme	

Discretions Policy – Firefighters Pensions Scheme

Requests for Decisions under Firefighters Pension Scheme

Minutes of the Pensions Board

5. Conclusion

The Committee was able to confirm:

- That the system of internal control, governance and risk management in the Authority was adequate in identifying risks and allowing the Authority to understand the appropriate management of these risks.
- That there were no areas of significant duplication or omission in the systems of internal control, governance and risk management that had come to the Committee's attention, and had not been adequately resolved.

6. Sources of assurance

The Committee gained assurance in order to produce the above conclusion, from the following sources:

The work of Internal Audit

The Authority's Internal Auditors gave the following opinion in their Annual Report for 2015/16:

*Based on the work undertaken during the year and the implementation by management of the recommendations made, Internal Audit can provide *reasonable assurance that the Fire Authority has adequate and effective governance, risk management and internal control processes. *We are pleased to report that this is an unqualified opinion and the highest level of assurance available to Audit Services. In giving our opinion it should be noted that assurance can never be absolute. The most that internal audit can provide is reasonable assurance that there are no major weaknesses in the Authority's governance, risk management and control processes".*

The work of the External Auditors

During the year the external auditors (Grant Thornton) reported back to the Audit Committee on a number of occasions as detailed in section 4 above. No issues of any significant concern were raised.

The Governance Statement

The Governance Statement operated throughout the year ended 31 March 2016 and up to the date of the approval of the annual report and accounts.

The systems to ensure the management of the risks have been shown to be sound.

Risk Management
The Committee regularly receives and reviews the Authority's Corporate Risk Register, and assesses the assurance provided in order to demonstrate how risks are being mitigated.

7. The Committee's main achievements

The Committee believes its key achievements during the year were:-

- Continuing to build a good working relationship with the Authority's new external auditors Grant Thornton.
- Receiving and reviewing a number of useful sector updates from the external auditors.
- Following the final abolition of the Audit Commission, continuing to maintain an awareness of the likely changes to the appointment of external auditors through the Local Audit and Accountability Act.
- Reviewing the Committee's Terms of Reference in order to ensure they remain fit for purpose.
- Providing additional assurance through a process of on-going independent review.
- Raising the profile of internal control issues across the Authority and of the need to ensure that audit recommendations are implemented.
- Regular consideration and review of the Authority's Risk Register and accompanying assurances.
- Building the skills and knowledge of Committee members through regular technical updates and the consideration of related guidance issued by CIPFA.
- The continued presence of an independent member in order to broaden the Committee's experience and independent view point.

Appendix A

Terms of Reference for the Committee

Terms of Reference were reviewed in order to ensure that they remained fit for purpose, and that they reflected guidance provided in the Chartered Institute of Public Finance and Accountancy (CIPFA) Audit Committees – Practical Guidance for Local Authorities 2013 Edition:

Statement of purpose

Our Audit Committee is a key component of the Authority's corporate governance. It provides an independent and high-level focus on the audit, assurance and reporting arrangements that underpin good governance and financial standards.

The purpose of our Audit Committee is to provide independent assurance to the Members of the adequacy of the risk management framework and the internal control environment. It provides independent review of the governance, risk management and control frameworks and oversees the financial reporting and annual governance processers. It oversees internal audit and external audit, helping to ensure efficient and effective assurance arrangements are in place.

Governance, risk and control

To review the Authority's corporate governance arrangements against the good governance framework and consider annual governance reports and assurances.

To review the annual governance statement prior to approval and consider whether it properly reflects the risk environment and supporting assurances, taking into account internal audit's opinion on the overall adequacy and effectiveness of the Authority's framework of governance, risk management and control.

To consider the Authority's arrangements to secure value for money and review assurances and assessments on the effectiveness of these arrangements.

To consider the Authority's framework of assurance and ensure that it adequately addresses the risks and priorities of the Authority.

To monitor the effective development and operation of risk management in the Authority.

To monitor progress in addressing risk-related issues reported to the Committee.

To consider reports on the effectiveness of internal controls and monitor the implementation of agreed actions.

To review the assessment of fraud risks and potential harm to the Authority from fraud and corruption.

To monitor the counter-fraud strategy, actions and resources.

Internal Audit

To approve the internal audit charter.

To review proposals made in relation to the appointment of external providers of internal audit services and to make recommendations.

To approve risk based internal audit plan, including internal audit's resource requirements, the approach to using other sources of assurance and any work required to place reliance upon those other sources.

To approve significant interim changes to the risk-based internal audit plan and resource requirements.

To make appropriate enquiries of both management and the head of internal audit to determine if there are any inappropriate scope or resource limitations.

To consider reports from the head of internal audit on internal audit's performance during the year, including the performance of external providers of internal audit services. These will include:

- Updates on the work of internal audit including key findings, issues of concern and action in hand as a result of internal audit work;
- Regular reports on the results of the quality assurance and improvement programme;
- Reports on instances where the internal audit function does not conform to the Public Sector Internal Audit Standards and Local Government Application Note, considering whether the non-conformance is significant enough that it must be included in the annual governance statement.

To consider the head of internal audit's annual report:

- The statement of the level of conformance with the Public Sector Internal Audit Standards and Local Government Application Note and the results of the quality assurance and improvement programme that supports the statement - these will indicate the reliability of the conclusions of internal audit.
- The opinion on the overall adequacy and effectiveness of the Authority's framework of governance, risk management and control together with the summary of the work supporting the opinion - these will assist the committee in reviewing the annual governance statement.

To consider summaries of specific internal audit reports as requested.

To receive reports outlining the action taken where the head of internal audit has concluded that management has accepted a level of risk that may be unacceptable to the authority or there are concerns about progress with the implementation of agreed actions.

To contribute to the quality assurance and improvement programme and in particular, to the external quality assessment of internal audit that takes place at least once every five years.

To consider a report on the effectiveness of internal audit to support the annual governance statement, where required to do so by the Accounts and Audit Regulations.

To support the development of effective communication with the head of internal audit.

External Audit (Grant Thornton)

To consider the external auditor's annual letter, relevant reports, and the report to those charged with governance.

To consider specific reports as agreed with the external auditor.

To comment on the scope and depth of external audit work and to ensure it gives value for money.

To commission work from internal and external audit.

To advise and recommend on the effectiveness of relationships between external and internal audit and other inspection agencies or relevant bodies.

Financial Reporting

To review the annual statement of accounts. Specifically, to consider whether appropriate accounting policies have been followed and whether there are concerns arising from the financial statements or from the audit that need to be brought to the attention of the Authority.

To consider the external auditor's report to those charged with governance on issues arising from the audit of the accounts.

Accountability arrangements

To report to those charged with governance on the Committee's findings, conclusions and recommendations concerning the adequacy and effectiveness of their governance, risk management and internal control frameworks, financial reporting arrangements, and internal and external audit functions.

To report to full Authority on a regular basis on the Committee's performance in relation to the terms of reference, and the effectiveness of the Committee in meeting its purpose.

WEST MIDLANDS FIRE AND RESCUE AUTHORITY

AUDIT COMMITTEE
WORK PROGRAMME 2015/16

Date of Meeting	Item	Responsible Officer	Completed
2015			
29 June [Authority]	Annual Report of the Audit Committee 2014/15	Chair	
7 September	Corporate Risk 2015/16 – Quarter 1 Treasury Management Annual Report 2014/15 CIPFA Audit Committee Update Minutes and Terms of Reference of the Pensions Board Decisions on Discretions to Firefighter Pension Scheme Work Programme 2015/16	Director of Service Support Treasurer Audit Manager Chair of the Pensions Board Pension and Payroll Manager Democratic Officer	
21 September [Authority]	Audit Issues 2014/15 Approval of Statement of Accounts 2014/2015	Grant Thornton Treasurer	

9 November 2015	Quarter 1 Internal Audit Progress Report Treasury Management – Mid year review 2015/16 Audit Committee – Knowledge and Skills Framework External Audit progress Report Value for Money Report 2014/15 Annual Audit Letter 2014/15	Audit Manager Treasurer Audit Manager Grant Thornton Grant Thornton Grant Thornton	
November	*Corporate Risk Management Training*	Strategic Hub	
2016			
18 January	Quarter 2 Internal Audit Progress Report Internal Audit Charter – Annual Review CIPFA Audit Committee Update No. 18 Quarter 2 Corporate Risk Report Evaluating the effectiveness of the Audit Committee	Audit Manager Audit Manager Audit Manager Director of Service Support Audit Manager	

	External Audit Committee Update	Grant Thornton	
11 April	External Audit Committee Update for WMFRA Communication with the Audit Committee for WMFRA Audit Plan 2015/16 Quarter 3 Internal Audit Progress Report at 31.1.16 Internal Audit Plan 2016/17 Audit Committee Terms of Reference External Audit Work Programme and Scale of Fees Frequency of Corporate Risk Reporting to Audit Committee Corporate Risk Report Quarter 3 Update 2015/16 Minutes of the Pensions Board *Committee Members' Private meeting with Internal Auditors (to follow Committee)*	Grant Thornton Grant Thornton Grant Thornton Audit Manager Audit Manager Audit Manager Director of Service Support Director of Service Support Chair of the Pensions Board *Audit Manager*	
6 June	Annual Internal Audit Report Consider Governance Statement Annual Whistleblowing Report	Audit Manager Treasurer Monitoring Officer/Director of	

		Service Support	
	Annual Report of the Audit Committee	Chair	
	Corporate Risk Audit Committee Report	Director of Service Support	
	Audit Committee Update	Grant Thornton	
	Committee Members' Private meeting with External Auditors	*Grant Thornton*	
	Workshop for Members on Statement of Accounts	*Treasurer*	
27 June [Authority]	Approval of the Governance Statement 2014/2015	Treasurer	
	Audit Committee – Terms of Reference, Annual Review (will now be reported to the Authority's AGM)	Audit Manager	
25 July 2015	Audit Committee Skills Audit	Audit Manager	