

# Buckinghamshire & Milton Keynes Fire Authority



<b>MEETING</b>	Overview and Audit Committee
<b>DATE OF MEETING</b>	22 July 2020
<b>OFFICER</b>	Mark Hemming – Director of Finance and Assets Maggie Gibb – Internal Audit Manager
<b>LEAD MEMBER</b>	Chairman of the Overview and Audit Committee
<b>SUBJECT OF THE REPORT</b>	<b>Annual Audit Report 2019/20</b>
<b>EXECUTIVE SUMMARY</b>	<p>To present the Annual Audit Report to the Overview and Audit Committee.</p> <p>In line with best practice, an annual report on the internal control environment is presented to those charged with governance.</p> <p>The Chief Internal Auditor's opinion is that the Fire Authority's system of internal control and risk management facilitates the effective exercise of the Authority's functions. This provides <b>Reasonable</b> assurance regarding the effective efficient and economic exercise of the Authority's functions.</p> <p>This opinion is reflected in the Annual Governance Statement.</p>
<b>ACTION</b>	Noting
<b>RECOMMENDATIONS</b>	It is recommended that Members review and note the contents of the Annual Report.
<b>RISK MANAGEMENT</b>	There are no risk implications arising from this report.
<b>FINANCIAL IMPLICATIONS</b>	The audit work was contained within the 2019/20 budget.
<b>LEGAL IMPLICATIONS</b>	There are no legal implications arising from this report.
<b>CONSISTENCY WITH THE PRINCIPLES OF THE DUTY TO COLLABORATE</b>	Not applicable.

Internal Audit Report: Annual Audit Report 2019/20

<b>HEALTH AND SAFETY</b>	There are no health and safety implications arising from this report.
<b>EQUALITY AND DIVERSITY</b>	There are no equality and diversity implications arising from this report.
<b>USE OF RESOURCES</b>	Communication and progress monitoring All audits, follow up reports and further updates will be submitted to SMB and Overview and Audit Committee.
<b>PROVENANCE SECTION &amp; BACKGROUND PAPERS</b>	Internal Audit Plan 2019/20 Internal Audit reports taken to Overview and Audit Committee
<b>APPENDICES</b>	Appendix A – Annual Audit Report 2019/20
<b>TIME REQUIRED</b>	10 minutes.
<b>REPORT ORIGINATOR AND CONTACT</b>	Maggie Gibb – Internal Audit Manager <a href="mailto:Maggie.Gibb@buckinghamshire.gov.uk">Maggie.Gibb@buckinghamshire.gov.uk</a> 01296 387327

# Buckinghamshire & Milton Keynes Fire Authority



**Internal Audit Service  
Annual Report of the Chief Internal Auditor 2019/20**

**July 2020**

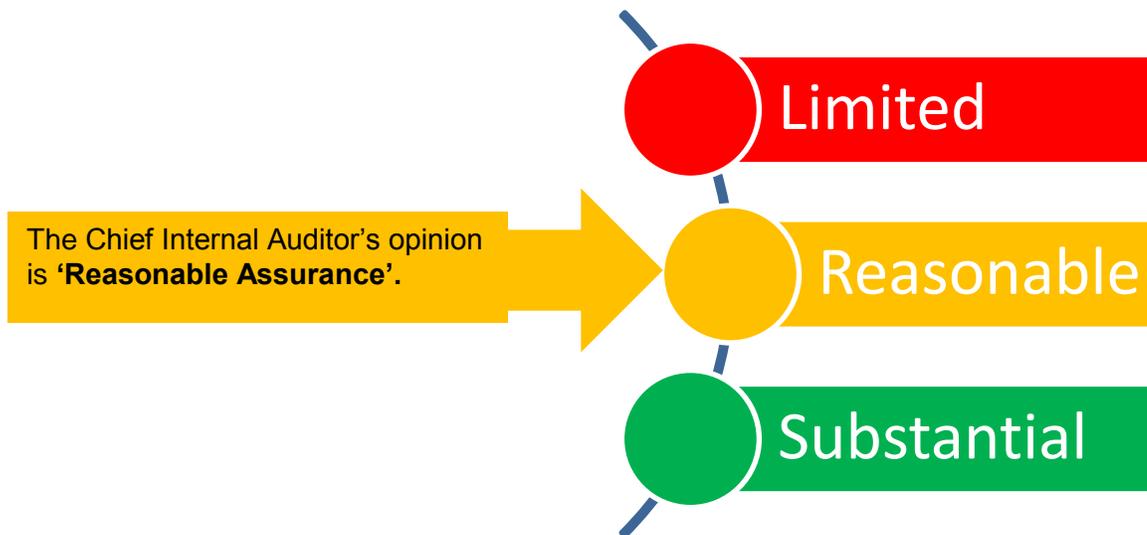
## 1. Introduction

- 1.1 This report outlines the Internal Audit work undertaken by the Internal Audit Service for the year ending 31 March 2020, and seeks to provide an opinion on the adequacy of the control environment detailing the incidences of any significant control failings or weaknesses.
- 1.2 The Account and Audit Regulations require the Fire Authority to maintain an adequate and effective Internal Audit Service in accordance with proper internal audit practices. The CIPFA Public Sector Internal Audit Standards (PSIAs), which sets out proper practice for Internal Audit, requires the Chief Internal Auditor to provide an annual report to those charged with governance, which should include an opinion on the overall adequacies of the internal control environment.

## 2. Responsibilities

- 2.1 The PSIA's define internal auditing as "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."
- 2.2 Internal Audit is not responsible for the control system. It is a management responsibility to develop and maintain the internal control framework and to ensure compliance. It is the responsibility of Internal Audit to form an independent opinion on the adequacy of the system of internal control. This opinion should be used as a key strand of the assurance framework which management use to develop their Annual Governance Statement.
- 2.3 The role of the internal audit service is to provide management with an objective assessment of whether systems and controls are working properly. It is a key part of the Authority's internal control system because it measures and evaluates the adequacy and effectiveness of other controls so that:
- The Fire Authority can establish the extent to which they can rely on the whole system; and
  - Individual managers can establish how reliable the systems and controls for which they are responsible are.

### 3. Chief Internal Auditor Opinion



*\* See Appendix 3 for definitions of the assurance opinions.*

3.1 Based on the audit work undertaken, our experience and knowledge of previous years' performance and the current climate in which the Authority is operating, in my opinion the system of internal control provides reasonable assurance regarding the effective, efficient and economic exercise of the Authority's functions. Findings raised from the 2019/20 internal audit reviews have not identified any material weaknesses to the internal control framework. Overall, the Fire Authority has continued to demonstrate a robust and effective internal control and risk management environment.

3.2 The Chief Internal Auditor would like to acknowledge the report from Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS) issued in December 2019 which concluded that the Fire Authority 'requires Improvement'. It should be noted that the conclusion of the inspection does not impact on my opinion on the adequacy and effectiveness of the Authority's internal control framework. However it should be recognised that the inspection has highlighted some fundamental risks that may impact the Authority's ability to achieve objectives. The Chief Internal Auditor is confident that Senior Officers in the Authority take the inspection findings seriously and with a strong improvement programme, clear deadlines and a robust governance framework which includes the Overview and Audit Committee scrutiny, the identified weaknesses will be addressed.

## 4. Basis of Audit Opinion

4.1 The Internal Audit Service operates in accordance with the Public Sector Internal Audit Standards (PSIAs). The Audit Strategy complies with the PSIAs and is summarised within the Service Level Agreement. This requires Internal Audit to objectively examine, evaluate and report on the adequacy of internal control as a contribution to the proper, economic, efficient and effective use of resources.

4.2 The Internal Audit Plan was developed in consultation with the Director of Finance and Assets to focus specifically on financial management, corporate processes and key risk areas. There were no constraints placed on the scope of audit work in the year and there were sufficient resources to provide an adequate and effective audit coverage. The Internal Audit Plan was approved by the Overview and Audit Committee.

4.3 The strategy for delivery of the Internal Audit Service is reviewed triennially and subject to the approval of the Overview and Audit Committee.

4.4 In arriving at our opinion, we have taken into account:

- The results of all audits undertaken as part of the 2019/20 Internal Audit Plan- **Appendix 1.**
- The results of follow-up action taken in respect of audits from previous years **Appendix 2.**
- Whether or not any 'high' priority recommendations have not been accepted by management and the consequent risks.
- The effects of any material changes in the Authority's objectives or activities.
- Whether or not any limitations have been placed on the scope of internal audit.
- Findings of work performed by other assurance providers (e.g. the External Auditors who we have liaised with throughout the year in order to share information and reduce any duplication of audit activity).
- The scope of the internal control environment - which comprises the whole framework of systems and controls established to manage BMKFRS to ensure that its objectives are met.

4.5 It should be noted that the Chief Internal Auditor opinion does not imply that Internal Audit has reviewed **all** risks relating to the Fire Authority. The most that the Internal Audit Service can provide to the Accountable Officers and Overview and Audit Committee is a **reasonable** assurance that there are no major weaknesses in control processes. The matters raised in this report are only those which came to our attention during our internal audit work and are not necessarily a comprehensive statement of all the weaknesses that exist, or of all the improvements that may be required.

## 5. Anti-Fraud

5.1 There have been no suspected frauds or financial irregularity brought to the attention of the Chief Internal Auditor during 2019/20. Throughout the year we continued to work closely with the Director of Finance and Assets on fraud awareness and our work on the core financial systems included a review of the key anti-fraud controls.

## 6. The Internal Audit Team

6.1 The Internal Audit Service is provided by the Business Assurance Team at Buckinghamshire Council. All staff are qualified or part-qualified with either ACCA, CIIA, QICA or AAT qualifications, and all audit work is subject to a rigorous quality assurance process.

6.2 The quality of work is assured through the close supervision of staff and the subsequent review of reports, audit files and working papers by an Audit Manager. Exit meetings are held with the relevant officers to ensure factual accuracy of findings and subsequent reporting, and to agree appropriate action where additional risk mitigation is required.

## 7. Our Performance

7.1 With effect from 1 April 2013, the Public Sector Internal Audit Standards were introduced as mandatory guidance that constitutes the principles of the fundamental requirements for the professional practice of internal auditing within the public sector.

7.2 We continue to monitor our performance standards as outlined in the service level agreement. This includes ensuring requests for assistance with suspected cases of fraud (% of responses made within 24 working hours) as appropriate and also monitor relationship management issues in the areas of:

- Timeliness
- Willingness to cooperate/helpfulness
- Responsiveness
- Methodical approach to dealing with requests
- Quality of work/service provided

7.3 The 2019/20 Internal Audit Strategy set out seven performance indicators that the Internal Audit Service was measured against. Below is a summary of our performance against the set indicators:

Performance Measure	Target	Method	19/20 Results
Elapsed time between start of the audit (opening meeting) and Exit Meeting.	Target date agreed for each assignment by the Audit manager, stated on Terms of Reference, but should be no more than 3 X the total audit assignment days (excepting annual leave etc.)	Internal Audit Performance Monitoring System	80%
Elapsed Time for completion of audit work (exit meeting) to issue of draft report.	15 Days	Internal Audit Performance Monitoring System	80%
Elapsed Time between issue of Draft report and issue of Final Report	15 Days	Internal Audit Performance Monitoring System	*100%
% of Internal Audit Planned Activity delivered by 30 April 2019	100% of Plan by End of April 2019	Internal Audit Performance Monitoring System	80%
% of High and Medium priority recommendations followed up after implementation date	All High and Medium recommendations followed up within three months of the date of expected implementation	Internal Audit Performance Monitoring System	100%
Customer satisfaction questionnaire (Audit Assignments)	Overall customer satisfaction 95%	Questionnaire	**Nil – questionnaires not utilised for this year

\* Please note that measure looks as the timeliness of reporting by the team, and delays caused by the auditees are not factored in.

\*\* Whilst questionnaires were not utilised for 19/20, feedback was provided on completion of each audit and is also discussed as part of the regular meetings with the Director of Finance & Assets.

It should be noted that due to Covid-19 a number of internal auditors were re-deployed to support the response to the pandemic. As a result two audits were delayed and were not completed within the planned timescales. However these delays were communicated and agreed with the Director of Finance and Assets.

***Maggie Gibb***

*Chief Internal Auditor*

*July 2020*

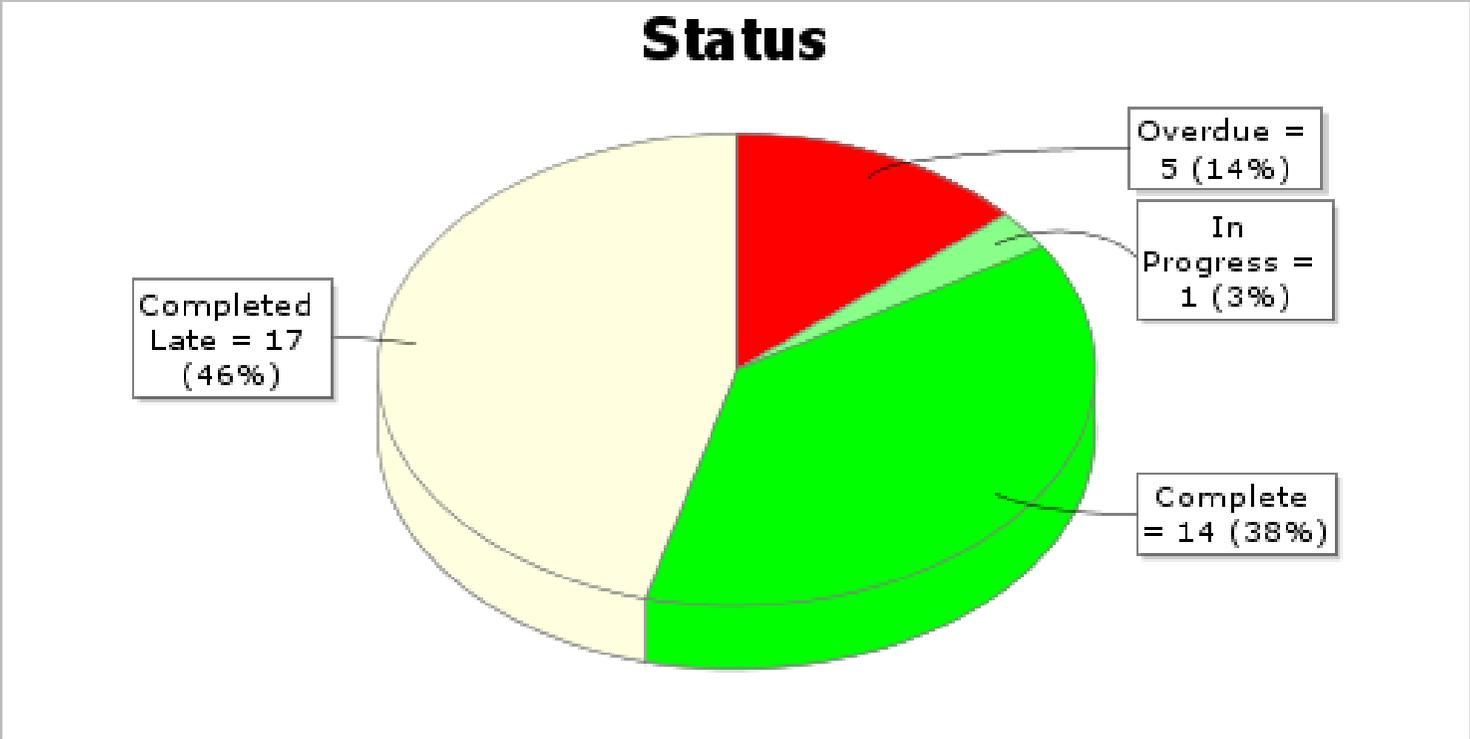
## Appendix 1: Summary of 2019/20 Audits Performed Informing the Annual Opinion

Audit Assignment (No. Days)	Audit Opinion	No. of Audit Actions by Priority	Summary of Audit Findings
Core Financial Controls (40 Days)	Substantial	<p>High = 0 Medium = 0 Low = 3</p>	<p><b>1. : Creditors – Purchase Orders</b>  <b>Finding:</b> A list of purchase invoices was obtained from a Purchase Ledger Transaction Report. A sample of 25 invoices was tested. Audit noted one instance where a retrospective Purchase Order for £60,000 had been raised inappropriately. This was for a Professional Partner Subscription payment, and as this would have been known about before the payment was made, a purchase order should have been raised beforehand. The Finance Officer monitors and flags instances of invoices without a purchase order. However, there is a small number of recurring retrospective purchase orders which should be escalated.  <b>Risk:</b> If purchase orders are raised retrospectively there is a risk that inappropriate purchases may be made and financial commitments are made outside of the Integra system which may lead to budget monitoring being inaccurate.</p> <p><b>2. Debtors – Reason for raising Credit Notes</b>  <b>Finding:</b> Examination of a sample of five credit notes raised between April 2019 and December 2019 found that in one case the reason for raising the credit note was not clear. The reason was recorded on Integra as ‘credit for invoice’ which did not sufficiently explain why a credit note was raised against the invoice payment. Whilst the value of credit notes is reviewed by the Principal Accountant as part of the Debt Management Control reconciliation, there was no evidence of independent monitoring of each credit note transaction.  <b>Risk:</b> If a sufficient and clear reason for raising a credit note is not recorded on Integra, there is a risk that the credit note has been raised inappropriately or in error, leading to financial loss to the Fire Authority.</p> <p><b>3. Payroll – Voluntary deductions</b>  <b>Finding:</b> Examination of a sample of 20 employees paid in December 2019 found the following exceptions:</p> <ul style="list-style-type: none"> <li>• In three cases where a deduction was recorded on the employee’s payslip for the Fire Authority’s prize draw, there was no prize draw deduction form held on file.</li> <li>• In one case where a charity deduction was recorded on the employee’s payslip, there was no charity deduction form held on file.</li> </ul> <p><b>Risk:</b> If authorisation to make a deduction from an employee’s payslip is not retained on file, there is a risk that a deduction to pay is made without the employee’s consent.</p>

Audit Assignment	Audit Opinion	No. of Audit Actions by Priority	Summary of Audit Findings
Performance Management	Reasonable	<p>High = 0  Medium = 2  Low = 2</p>	<p><b><u>1. Corporate Performance Framework – Customer Satisfaction Performance Measure (Medium)</u></b></p> <p><b>Finding:</b> A review of the Annual Performance Monitor 2018-2019 report showed that for the 'Customer Satisfaction' performance measure, the customer satisfaction results does not give any detail as to why customers are satisfied or dis-satisfied. The annual report also notes that “from this feedback [Customer Satisfaction] it would appear that it is not linked to the time taken by the Service to have an appliance on scene”. However, the strategic objective relating to the Customer Satisfaction performance measure is 'to provide a timely and proportionate response to incidents by allocating our assets and resources in relation to risk and demand'.</p> <p><b>Risk:</b> Given the lack of detail around the customer satisfaction results and its link to the strategic objective and what is stated in the annual report, there is a risk that management cannot make informed decisions that will impact on strategic objectives being achieved.</p> <p><b><u>2. Corporate Performance Framework – Council Tax Performance Measure (Medium)</u></b></p> <p><b>Finding:</b> One of the strategic objectives for the Fire Authority is to 'Offer best value for money to our residents and businesses' and one of the outcome measures against this strategic objective is “Council Tax rates compared with family group and / or other Combined Fire Authorities'.</p> <p>However, HMICFRS report issued in December 2019 states that the Fire Authority 'requires Improvement'. One of the questions asked was 'How efficient is the service at keeping people safe and secure?' and the following was noted by HMICFRS:</p> <p>“We have serious concerns as to whether Buckinghamshire FRS has the resources it needs to meet its foreseeable risk. As a result of the financial position the service finds itself in, it does not have enough operational firefighters to resource its prevention and protection functions and crew the minimum number of fire engines it says it needs.”</p> <p>Given that the Fire Authority must address the findings in the HMICFRS report to ensure that budget requirements and funding are sustainable in the future, it is no longer an appropriate performance measure that Buckinghamshire and Milton Keynes Fire Authority continues to be the lowest precepting Combined Fire Authority based on Band D Council Tax.</p> <p><b>Risk:</b> By not having appropriate performance measures in place there is a risk that management cannot make informed decisions that will impact on strategic objectives.</p> <p><b><u>3. Corporate Performance Framework – Bucks Fire &amp; Rescue Service (BRFS) Balance Scorecard (Low)</u></b></p> <p><b>Finding:</b> The Bucks Fire &amp; Rescue Service (BRFS) Balance Scorecard supplements the Fire Authority's Annual Performance Monitor report and details some of the performance measures from the Corporate Plan and are grouped into the following four quadrants; Prevention, Protection, Response and Finance. It was noted that on the BRFS Balance Scorecard, there are no headings to describe what each quadrant is showing the reader and how it relates back to strategic objectives.</p> <p><b>Risk:</b> If there are no appropriate headings or commentary alongside the balance scorecard, management may not be able to easily identify the link between performance and objectives.</p>

Audit Assignment	Audit Opinion	No. of Audit Actions by Priority	Summary of Audit Findings
Performance Management	Reasonable	<p>High = 0 Medium = 2 Low = 2</p>	<p><b><u>4. Risk and Performance Management – Risk Management Policy (Low)</u></b></p> <p><b>Finding:</b> The Risk Management Policy was last updated in 2015 and was approved by the Executive Committee on 18 March 2015. It is noted on the policy that it was due to be reviewed January 2018. However, the policy has yet to be reviewed.</p> <p><b>Risk:</b> If there is an out of date Risk Management Policy, there is a risk that the risk management processes are not effective to ensure performance meets strategic objectives.</p>
Cyber Security	Reasonable	<p>High = 0 Medium = 2 Low = 1</p>	<p><b><u>1. Role profiles and tidying up of current access permissions (Medium)</u></b></p> <p><b>Finding:</b> Role profiles have not been identified and are therefore not in use. We note that access rights have been created and some users have additional privileges granted after the initial user permissions have been created. User profiles therefore need to be reviewed to ensure that there is a business need for all users to access the systems and date they have been granted, however this has not been completed.</p> <p><b>Risk:</b> This increases the risk of unauthorised access being granted as there is no set profile structure, which could result in users having access to data they are not entitled to view.</p> <p><b><u>2. Training and the measurement of its effectiveness (Medium)</u></b></p> <p><b>Finding:</b> At the time of the audit, 92.3% of all staff had completed mandatory e-Learning security training “Protecting Information”. This training is provided as part of the user induction process.</p> <p>All training materials and relevant topic updates are added to the Intranet, however there is not a standard cyber security refresher course, and no mock phishing attacks are completed to test the effectiveness of induction training and user awareness.</p> <p><b>Risk:</b> This increases the risk of users not being aware of, or accountable for inappropriate use of the Authority’s devices, which could result in a cyber-attack or data breach occurring.</p> <p><b><u>3. Contract management with Udata (Low)</u></b></p> <p><b>Finding:</b> The network is managed by Udata with support from the Authority. The Operational Process document agreed with Udata sets out target response times, and states that monthly service performance reports will be sent to the Authority on the 10<sup>th</sup> working day of the calendar month. The reports should include incidents raised, analysis of resolution categories, time to fix, performance to SLA and service availability. These reports are not provided by Udata.</p> <p><b>Risk:</b> There is an increased risk that Udata are not effectively delivering against their SLA targets, and this may not be identified. There is also a risk that the overall high level monitoring of network issues is not identified.</p>
Budget Monitoring and Forecasting	Substantial	<p>High = 0 Medium = 0 Low = 0</p>	<p>All control areas reviewed were found to be adequate and no recommendations were raised as a sound system of internal control designed to achieve objectives and minimise risk was found to be in place and operating effectively.</p>

Appendix 2: Current Status of Audit Actions as at 20 June 2019



\* This is a summary status of all audit recommendations raised from 2017/18 to date.

## Detailed Description of Overdue Audit Actions as at 20 June 2019

Title	Priority	Due Date	Description	Latest Note
<p>Fleet Management (1a &amp; b) Tranman Review</p>	<p>Medium Priority</p>	<p>31-Aug-2017</p>	<p><b>Finding</b>                      In discussion with the Fleet Manager it was confirmed that the latest Tranman training was delivered circa. December 2015 through a one day training event. This training event covered a large amount of materials in a short period of time and meant that a number of key topics were not covered in their entirety or in sufficient detail to fully absorbed the information to the required standard.                      Since the training was delivered there have also been a number of staff changes, resulting in three members of staff, from a five person team who use the Tranman system, never being taught the full system and how to use the software from the software provider. This has led to potential under-utilisation of the software and some inconsistencies in the use of the system potentially compromising data integrity and alignment of processes.                      In addition it was noted that there are current reporting issues through the Crystal Reporting function, which added to the potential inconsistencies in the use of the system means reporting functions cannot be fully relied upon to provide up to date and valid information to base decisions upon. Audit acknowledges that the reporting issue is currently being investigated by Tranman.</p> <p><b>Risk</b>                      Where training is not provided on a periodic basis, staff may adopted inappropriate, ineffective, and / or out dated working practices.</p> <p><b>Action</b>                      1a) Tranman to carry out a review of the current system and its utilisation and offer options for further utilisation of the current system, available 'upgrades' and system improvements. This information can then be analysed to ascertain the most appropriate action.                      1b) Identify training requirements, system improvements and possible upgrades for implementation in 2018/19 (depending on funding requirements).</p>	<p>Update from J. Finden, Fleet Manager (June 2020):</p> <p>The situation with the fleet management system is still as in the previous update, but I can confirm the contract has recently been signed and an order raised for the upgrade.</p> <p>I have had the initial contact from the Tranman project leader who informed me that our upgrade is now on their calendar and will contact me when they are ready for more information from us. The initial estimate is the project should be underway in September.</p>
<p>BMKFA 1718 1830 Property Management (1) Red Kite Functionality</p>	<p>Low Priority</p>	<p>31-Mar-2020</p>	<p><b>Finding</b>                      Review of 10 Reactive Works jobs on Red Kite, identified two red rated jobs which were closed within 24 hours of the job being open, this cannot confirm whether it was made operationally safe within the four hour timeframe. There were also two Amber Rated jobs, one of which was closed within 72 Hours and the other 144 hours.</p> <p><b>Risk</b>                      Where the Authority are unable to hold record events as they become operationally safe, there is a lack of information available to confirm whether these internal targets are being consistently met.</p> <p><b>Action</b>                      As part of the latter phase of the BASI project it is intended to review the current asset management systems utilised by the Authority, part of this review will examine the case for improving the functionality of existing systems working with the suppliers to develop them accordingly. This work is currently scheduled for early 2019.</p>	<p>Update from Gordon Wylie, Property Manager (June 2020):</p> <p>There is no further progress since my last update. Covid 19 has effected what is essential and non-essential in terms of workloads. I do not see us returning to this until early 2021.</p>

Title	Priority	Due Date	Description	Latest Note
<p>BMKFA 1819 1947 Project Management BLH (2) The Hub Performance</p>	<p>Medium Priority</p>	<p>31-Oct- 2019</p>	<p><b>Finding</b> During the Audit it was confirmed that the HUB have had difficulties with technical support; which has had an impact of the timeliness of design work, changes or updates and which in turn has led to delays in providing information that is required by Kingerlee – the construction firm. The Quantity Surveyor maintains a schedule of delays caused by the HUB and the associated costs. It was confirmed that any financial implications that arise as a result of the HUB’s poor performance could potentially be recoverable. However Audit found that whilst these potentially recoverable costs are reflected in the Budget Monitoring Financial Statements, they are not separately identified as attributable to any party as this will be the subject of negotiation between all parties depending on final outcomes at the conclusion of construction. The risk of HUB poor performance has been recorded in the risk register. It was confirmed that the Director for the HUB Professional Services has been made aware of potentially recoverable costs and the issues that were causing poor performance have been addressed.</p> <p><b>Risk</b> Where the impact of poor performance is not completely and accurately reflected in the budget and/or risk register, this may lead to project overspend as the budget will not be forecasting all expected costs.</p> <p><b>Action</b> The necessary actions to deal with potential financial loss arising from delays on the part of HUB have already been addressed during 2018 and a significant improvement has been seen. The current delay in the construction programme (5-6 weeks) has not altered for some months. Both the HUB and Kingerlee have a responsibility to mitigate any delay as much as possible and with some 8 months of construction still to take place at the time of writing (Feb 2019) they must both maintain the opportunity to do so. Only at post construction and during the period when the final account will be negotiated and agreed, will any financial loss due to delays or failures be attributed. The Director of HUB’s parent company (Integral UK Ltd) has been in discussions with both DFA and Property Manager and he is well aware of the potential claim the Authority may have in due course. The financial statements produced by the QS do show all costs (i.e. worst case) but do not at this stage set out which potentially claimable costs are attributable to which parties. The Authority’s officers will continue to maintain dialogue with senior representatives at both the HUB and Kingerlee over any potential situation (either worsening or improving) that may lead to a claim.</p>	<p>Update from Mark Hemming, Director of Finance and Assets (June 2020):</p> <p>Although practical completion of the building was achieved on 7 May 2020, there are still a number of matters outstanding before the final account can be agreed. It is anticipated that this will take place in the latter part of the year.</p>

Title	Priority	Due Date	Description	Latest Note
<p>BMKFA 1819 1948 Stores (2) Asset Review</p>	<p>High Priority</p>	<p>31- Dec- 2019</p>	<p><b>Finding</b> Staff are required to undertake regular asset checks. The frequency of these inventory checks are dependent on the type of items, with this being determined by the PIT Number each asset is assigned. When the staff check the assets, a device would be used to scan the tag label of each asset to show that the asset has been located and checked. Once the staff have scanned the item, evidence of this scan is registered automatically on Red Kite. During these inventory checks the staff will declare if they have found the asset and if it is inadequate or faulty. A sample of ten items was selected randomly from the Red Kite system. These were tested to see if the items had been checked in accordance with the frequency required. In two cases the location of the items was not found and the item had not been checked as a result.</p> <p><b>Risk</b> Where assets are not checked on a regular basis, there is a risk that faulty or inadequate items are being held and used by staff members.</p> <p><b>Action</b> Inventory checks should be reviewed by the Asset Management Systems Officer. Where the inventory checks have not been undertaken on a consistent basis, this will be followed up with staff.</p>	<p>Update from Maria Darrell, Asset Management and Equipment Manager (June 2020):</p> <p>This action will be dependent on when we employ someone to carry out the actions required. I think we should set a review date for this for the 31st September if you are agreeable.</p>
<p>BMKFA 1920 2021 Cyber Security (2) Training and the measurement of its effectiveness</p>	<p>Medium Priority</p>	<p>31-Mar- 2020</p>	<p><b>Finding:</b> At the time of the audit, 92.3% of all staff had completed mandatory e-Learning security training "Protecting Information". This training is provided as part of the user induction process. All training materials and relevant topic updates are added to the Intranet, however there is not a standard cyber security refresher course, and no mock phishing attacks are completed to test the effectiveness of induction training and user awareness. We recommend that an annual refresher training course/package is completed and rolled out to all users to ensure that they are kept up to date with the most recent guidance. Mock phishing attacks should be scheduled on a rotational basis to establish the effectiveness of training and user awareness.</p> <p><b>Risk:</b> This increases the risk of users not being aware of, or accountable for inappropriate use of the Authority's devices, which could result in a cyber-attack or data breach occurring.</p> <p><b>Action:</b> The "Responsible for Information" general user is completed by all new starters and bi-annually by all employees via the HEAT package (an online training facility). It replaced the "Protecting Information" training. HEAT sends out reminders when the refresher training is due. It is proposed to maintain the refresher training as bi-annual (rather than annually as suggested). We are in discussion with BCC Audit for suggested mock phishing providers. We have identified a free cyber training package from the National Cyber Security Centre <a href="https://www.ncsc.gov.uk/training/top-tips-for-staff-web/story_html5.html">https://www.ncsc.gov.uk/training/top-tips-for-staff-web/story_html5.html</a> It is proposed to roll this out via HEAT with refreshers on a bi-annual basis by 31 March 2020 After the free training session provided by the South East Regional Organised Crime Unit to SMB on 1 October 2018 it was agreed that its free training offer for lower tier would be rolled out.</p>	<p>Update from Gerry Barry, Information Governance and Compliance Manager (June 2020):</p> <p>We have recently moved to a new "Heat" online training facility. All employees will complete "Responsible for Information" bi-annually and the National Cyber Security Centre's "Top tips for staff" cyber security training alternate years. Having investigated mock phishing attacks I find there are inconclusive benefits. The then Buckinghamshire County Council audit team were unable to provide me with details of the supplier / process they used for mock phishing attacks. The training offered by the SEROCU was arranged for Spring 2020 and had to be cancelled owing to the coronavirus pandemic. This will be rescheduled at a future date. Additional InfoSec training is delivered by the Information Governance &amp; Compliance Manager as part of Watch and Crew Manager development and also ad hoc training to individuals and teams to address specific issues.</p>

### Appendix 3 Definition of Assurance Opinions

For each audit an opinion was determined firstly on the framework of controls that exist for that operational area and secondly on compliance with the controls. From this an overall audit opinion is given for each audit. An opinion on the quality of risk management in place is also provided. Work has been planned and performed so as to obtain all the information and explanations which were considered necessary to provide sufficient evidence in forming an audit opinion. The range of audit opinions is:-

	<b>Limited</b>	The system of internal control is weak and risks are not being effectively managed. The system is open to the risk of significant error or abuse. Significant action is required to improve controls.
	<b>Reasonable</b>	There is generally a good system of internal control in place and the majority of risks are being effectively managed. However some action is required to improve controls.
	<b>Substantial</b>	There is a strong system of internal control in place and risks are being effectively managed. Some minor action may be required to improve controls.