Buckinghamshire & Milton Keynes Fire Authority

Meeting and date: Overview and Audit Committee, 21 July 2021

Report title: Internal Audit Report - Annual Audit Report 2020/21

Lead Member: Councillor David Carroll

Report sponsor: Mark Hemming – Director of Finance and Assets

Author and contact: Maggie Gibb – Internal Audit Manager, Maggie.Gibb@buckinghamshire.gov.uk, 01296 387327

Action: Noting.

Recommendations: It is recommended that Members review and note the contents of the Annual Audit Report.

Executive summary: To present the Annual Audit Report to the Overview and Audit Committee. In line with best practice, an annual report on the internal control environment is presented to those charged with governance.

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 **Reasonable** assurance regarding the effective efficient and economic exercise of the Authority's functions. This opinion is reflected in the Annual Governance Statement.

Financial implications: The audit work was contained within the 2020/21 budget.

Risk management: There are no risk implications arising from this report.

Legal implications: There are no legal implications arising from this report.

Privacy and security implications: There are no privacy and security implications arising from this report.

Duty to collaborate: Not applicable.

Health and safety implications: There are no health and safety implications arising from this report.

Environmental implications: There are no environmental implications arising from this report.

Equality, diversity, and inclusion implications: There are no equality and diversity implications arising from this report.

Consultation and communication: Not applicable.

Background papers:

Appendix	Title	Protective Marking
1	Annual Audit Report	Not applicable

Buckinghamshire & Milton Keynes Fire Authority

Internal Audit Service
Annual Report of the Chief Internal Auditor 2020/21

July 2021

1. Introduction

1.1 This report outlines the Internal Audit work undertaken by the Internal Audit Service for the year ending 31 March 2021 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

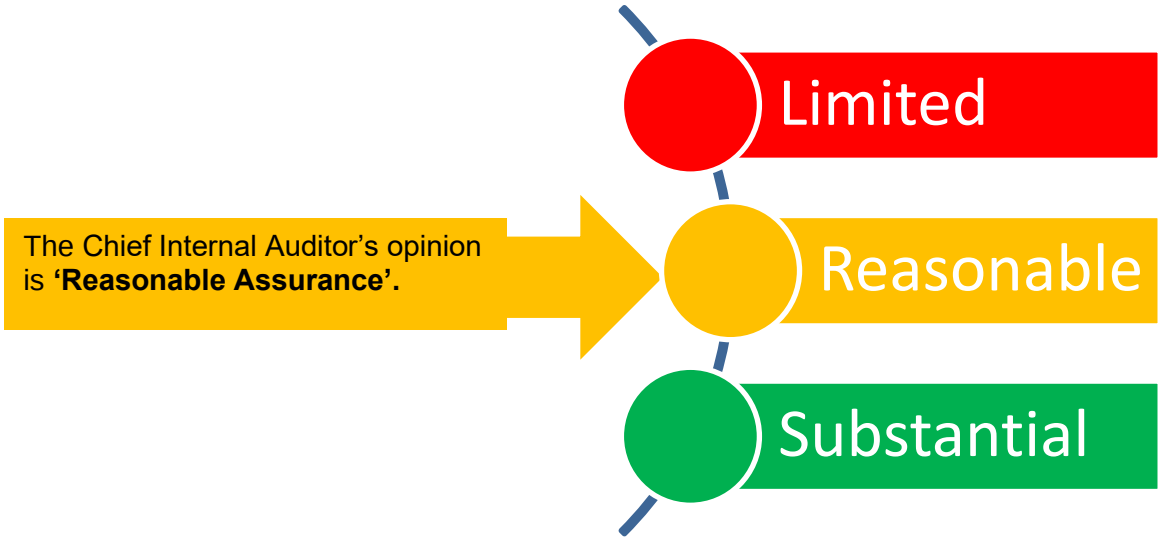
2.1 The PSIA's define internal auditing as "an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness 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. However, our work has identified further enhancements that are required to ensure that the internal control framework remains adequate and effective. Findings raised from the 2020/21 internal audit reviews have not identified any material weaknesses. 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 Fire Authority's response to Covid-19 and the business continuity measures that were put in place to ensure that statutory responsibilities were fulfilled during the pandemic. The robust governance framework in place ensured that decisions were approved accordingly and that risk implications were considered as part of the decision-making process. A Covid-19 inspection was undertaken by Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS); and the letter issued in January 20121 concluded that the Fire Authority 'responded well during the pandemic and provided additional support to its communities'. It should be noted that the Fire Authority has continued to work on the improvement plan which was developed to address the recommendations raised by HMICFRS in December 2019 which highlighted some fundamental risks to the authority.

The Chief Internal Auditor remains confident that the identified weakness from the inspection will be addressed through the strong improvement programme and a robust governance framework which includes the Overview and Audit Committee scrutiny.

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 controls 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, however it should be recognised that due to the pandemic the majority of the audit plan was delivered through remote auditing with an increased reliance on officers providing the documentation to auditors electronically and demonstrating processes via screen-sharing.

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 2020/21 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 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 2020/21 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	2020/21 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	**100%**
% 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 this year, 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 we had two audits delayed and were not completed within the planned timescales. This was due to the internal auditors being re-deployed to support the response to the pandemic; and staff illness due to Covid. All delays were communicated and agreed with the Director of Finance and Assets.

Maggie Gibb

Chief Internal Auditor

July 2021

Appendix 1: Summary of 2020/21 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	High = 0 Medium = 2 Low = 1	**1. Payroll – Authorisation of CPD payments (MEDIUM)** **Finding:** Examination of a sample of 10 permanent changes made to Payroll between April and November 2020 found that in one case, authorisation from a line manager or Director was not held on file. This case involved the addition of CPD payments for an employee following an email from the Training, Learning & Development Assistant. The Payroll and Benefits Manager established that a review of CPD is ongoing. It was agreed through discussion with the Payroll and Benefits Manager that the Line Manager or Budget Holder should be copied in on CPD requests received from OD. Any CPD input should be confirmed with them at the point of processing. **Risk:** If additional recurring payments are actioned on the Payroll system without authorisation from the Line Manager or Budget holder, there is a risk that the employee is not entitled to the payment, leading to unexpected additional expenditure for the Department in which they work and increasing the risk that an overpayment is made to the employee, resulting in a financial loss to the Fire Authority. **2. Payroll – Flow of information from HR to Payroll during Leaver and Change of Role processes (MEDIUM)** **Finding:** Examination of a sample of 10 employees who left the Fire Authority's employment between April and November 2020 found that four leaver notifications were received by Payroll after the leave date. Three of these were received after the payroll cut off for that month. In one case this led to the creation of an overpayment. Discussion with the Payroll and Benefits Manager established that the Leaver process changed during 2019-20. Line managers no longer advised Payroll directly of Leavers. The amended process involves line managers advising HR and HR passing Leaver information on to Payroll. Following iTrent permission changes, Payroll can no longer process Leavers if HR does not have the capacity to or in the event of late leavers after the Payroll cut-off. The result of these process changes is that information reaches Payroll last, sometimes after the employee has already left the organisation, reducing Payroll's ability to address the risk of overpayments. To mitigate overpayments, Payroll manually adjusts pay within the record whilst it is still live. Payroll is more reliant on manual intervention and affects their timeliness in reporting to HMRC. Examination of a sample of ten On-Call and Overtime payments made to staff between April and November 2020 found one case where a request was submitted via email. This was due to a discrepancy with a change in role and a change in Terms and Conditions for the employee. Not all of the necessary managers were involved in this process, and contractual changes were not communicated effectively. This resulted in an overpayment. Corrective action was taken by the employee's line manager and Payroll. **Risk:** If Payroll is not provided with complete and timely information to process Leavers and role changes, there is a risk that Leavers and pay implications of role changes are not actioned on iTrent before Payroll being run, leading to the creation of an overpayment and financial loss to the Fire Authority.

Audit Assignment	Audit Opinion	No. of Audit Actions by Priority	Summary of Audit Findings
Core Financial Controls (40 Days	Substantial	High = 0 Medium = 2 Low = 1	**3. Creditors - Timely removal of Finance system access (LOW)** **Finding:** A staff member was listed as an active Integra user in November 2020 despite having retired from the organisation in June 2020. Although the role was not linked to a cost centre and the former employee would have had no physical access to Integra due to the system only being accessible via the Fire Authority's internal servers, it is good practice to update all data sets for staff changes, as inactive accounts pose a security risk and are a potential target for hackers. From testing we found that one former employee was listed as a P-Card user registered with Lloyds bank and was still listed as a user on Integra. It was confirmed that there was no continuing access to the card, and it had been deactivated on Integra. Therefore if there was any spend on the purchasing card, this would have been flagged as part of the process of uploading the purchasing card statement from Lloyds into Integra. **Risk:** If P-Card and Integra user access is not removed in a timely manner following the leave date, there is a risk that unauthorised spending is incurred and that card fees are paid for unused cards, leading to financial loss to the Fire Authority.
GDPR	Partial	High = 1 Medium = 3 Low = 1	**1. Data Incidents and Reporting (HIGH)** **Finding:** During the audit fieldwork, the DPO confirmed that there had been no 'reportable breaches' at the Authority. However, after the audit fieldwork, a data breach incident was brought to Internal Audit's attention. The incident was related to an audit report for Staff Members' Equal Pay published within the Overview and Audit Committee agenda pack for the meeting dated 11 November 2020. Discussions with the Director of Finance and Assets confirmed that the report was accessed 20 times before being removed from the public website. An investigation was undertaken by the DPO raising 12 recommendations. The investigation required HR to identify all employees whose personally identifiable information has been published. Also, relevant Managers will be responsible for explaining that information has been released, measures taken, and those being taken to prevent further occurrences. **Risk:** If there is a lack of awareness of reporting for incidents, there is a risk that incidents are not identified and actioned promptly and a risk that reportable breaches are not reported to the ICO which may lead to fines. **2. E-learning modules (MEDIUM)** **Finding:** The Authority has a General Data Protection Regulation (GDPR) and a Cyber Security eLearning module implemented in April 2020. It runs at a two-year frequency for all staff. The People Systems and Learning Design Manager confirmed that as of December 2020, 103 (24%) staff members had completed both modules, and 324 (76%) had not. **Risk:** If an excessive period is granted to staff to complete training, there is a risk of an inconsistent approach to GDPR within the Authority, leading to breaches in legislation. **3. Records of Processing Activities (ROPAs (MEDIUM)** **Finding:** Departments within the Authority are also responsible for retaining their ROPA spreadsheets. However, the Safeguarding ROPA does not include all requirements stated by the ICO. This document did not specify whether it was a controller or a processor nor the retention schedules. **Risk:** If a centralised ROPA is held along with individual departmental ROPAs, the centralised ROPA is not kept up to date as the individual departmental ROPA's. If there is a lack of compliance checks, the risk of ROPAs not being kept up to date furthers.

Audit Assignment	Audit Opinion	No. of Audit Actions by Priority	Summary of Audit Findings
GDPR	Partial	High = 1 Medium = 3 Low = 1	**4. Retention and Destruction (MEDIUM)** **Finding:** The Information Governance and Compliance Manager is responsible for maintaining and reviewing records management processes. The retention schedules for departments and stations are defined within the ROPA. The Authority relies on stewards to ensure that electronic data is disposed of per the retention schedule. However, there is no mechanism in place to ensure this takes place **Risk:** If no adequate processes are in place to ensure lawful retention schedules and/or destruction of electronic records, there is a risk of accidental and/or unlawful alteration, destruction, or authorised personal data disclosure. **5. Procedures (LOW)** **Finding:** Review of procedures identified that the Data Quality procedure, Dealing with Requests for Information procedure and Redacting Sensitive Information Procedure referred to an Integrated Impact Assessment, which is no longer in place at the Authority. It was also identified that the Redacting Sensitive Information Procedure did not refer to when it was last reviewed and approved. **Risk:** Where policies and procedures are not reviewed regularly, there is a risk that staff guidance is not fit for purpose, which may lead to breaches in legislation.
Resource Management Application	Partial	High = 1 Medium = 5 Low = 2	**1. Service Reviews (HIGH)** **Finding:** Service reviews are held monthly with the Vendor as part of the managed service contract. It was noted that no formal documentation is provided as part of these service reviews and these reviews are held informally with discussions over the telephone. No formal minutes or documents are retained by the Authority. In addition, the FSR system is cloud based and hosted on behalf of the Authority by the Vendor. Commonly in such scenarios, user organisations (i.e. the Authority) would proactively require independent assurances from the service provider (i.e. the Vendor) in order to provide comfort that those controls outsourced to the service provider by the user organisation operate effectively and continue to maintain effectiveness as IT risks change or emerge. **Risk**: The organisation is wholly reliant on the Vendor for the service provided without any assurances that risks and controls are being managed effectively. A risk that materialises in relation to the service provider environment could potentially have an impact on the Authority's reputation (e.g. a cyber breach at FSR could result in the Authority data leakage). **2. Change Management – Internal Tracking and Assessment (MEDIUM)** **Finding:** The Authority was unable to provide any documentation around the selected changes for inspection. Therefore, we were unable to determine if the change management process had been followed for the selected changes. This included cost benefit analysis and CAB minutes of discussion. **Risk**: There is a risk of implementation of changes that contain bugs, misaligned with business requirements or impact on the continued operation of the production application. Development changes are misclassified, create unforeseen cost and/or are not assessed for business need and risk.

Audit Assignment	Audit Opinion	No. of Audit Actions by Priority	Summary of Audit Findings
Resource Management Application	Partial	High = 1 Medium = 5 Low = 2	**3. Joiners, Movers and Leavers Policy/Procedure (MEDIUM)** **Finding:** We noted that: • When a joiner or mover requires new access or a change in access, a ticket is raised in the Vivantio service desk. Within this ticket, a 'child ticket' is sent to the Resource Management Team (RMT) to create/amend the user's access. • This ticket does not capture sufficient information for the RMT operator to provide access. • Often users will be provided access and then request further access as this has not been initially provided. Therefore, access being granted is an iterative process. • The lack of information on the ticket reduces the effectiveness of the audit trail. • Previously, when a user left the organisation, residual access could be left on the account, this is due to there being no formal procedure when revoking access. • The process has slightly changed whereby an operator will look at the user account to check what access they have before removing it. **Risk:** Unauthorised access to company resources may lead to loss and compromise of data. **4. Generic Accounts (MEDIUM)** **Finding:** We inspected the user account list on FSR and noted that seven generic accounts exist on the FSR application as follows: • Five of these accounts have the username 'bucks_demoffX' where X is a number between 1-5. The use and rationale of these accounts was not provided by management; • One account with the username 'rmtcrashtestdummy' which similarly, was not rationalised; • One account has the username 'usardog'. It was noted that this account is created for the canine unit that the Urban Search and Rescue (USAR) team utilise. • It was further noted that the 5 'demoffX' accounts had never logged into FSR, the 'crashtestdummy' account was last accessed in May 2020. **Risk:** There could be a loss of accountability of user performed actions. Unauthorised access to company resources may lead to loss and compromise of data. **5. Backups – Disaster Recovery Testing (MEDIUM)** **Finding:** Although it was determined that backups are being conducted on the FSR application and that the Vendor are trained to conduct disaster recovery tests, no evidence was available to inspect to demonstrate a disaster recovery test had been performed. We recognise that this is often an annual exercise and FSR has only been in effect at the Authority since April 2020. **Risk:** There is a risk of partial or complete loss of data. Unavailability of systems and lack of business continuity.
Audit Assignment	Audit Opinion	No. of Audit Actions by Priority	Summary of Audit Findings

Resource Management Application	**Partial**	**High = 1** **Medium = 5** **Low = 2**	**6. Change Management - Testing Accounts (MEDIUM)** **Finding:** Testing noted the following: • The Authority does not have access to a test environment for FSR; • Changes are developed and tested by the Vendor; • Functional requirements and subsequent tender review for the application highlighted a question over access to a test environment to perform user acceptance testing (UAT) when a change is being made to the application; • Changes pass through over 1000 automated tests that are ran on the application to ensure that the change does not impact anything on the application, the change then has specific testing to ensure it is performing the functionality as per the design. • The Authority does not obtain any assurance from the vendor surrounding the change management process and is thus wholly reliant on the vendor for this. **Risk:** There is a risk that implementation of changes which are not aligned with business requirements and/or impact on the continued operation of the production application. Implementation of developments containing bugs or not matching the business' requirements. **7. User Access Reviews (LOW)** **Finding:** We noted that periodic user access reviews are not undertaken by the Resource Management Team at the authority when managing users access. Although a review of user access was completed in July 2020, there are no plans for this to continue. **Risk:** There is a risk of inappropriate access to the Authority's resources. **8. Password Configuration (LOW)** **Finding:** Fire service rota does not use traditional password configuration to manage passwords at a group level. FSR uses an 'entropy plugin' to set password configurations for all users which are set at 40 bits. Although 40 bits of entropy is considered 'reasonable' in regard to network and company passwords, full control over password parameters cannot be implemented as FSR (the application) does not allow for editing of password configuration. **Risk:** There is a risk of unauthorised access to company resources due to weak password configuration, which increases the likelihood of a brute force attack.

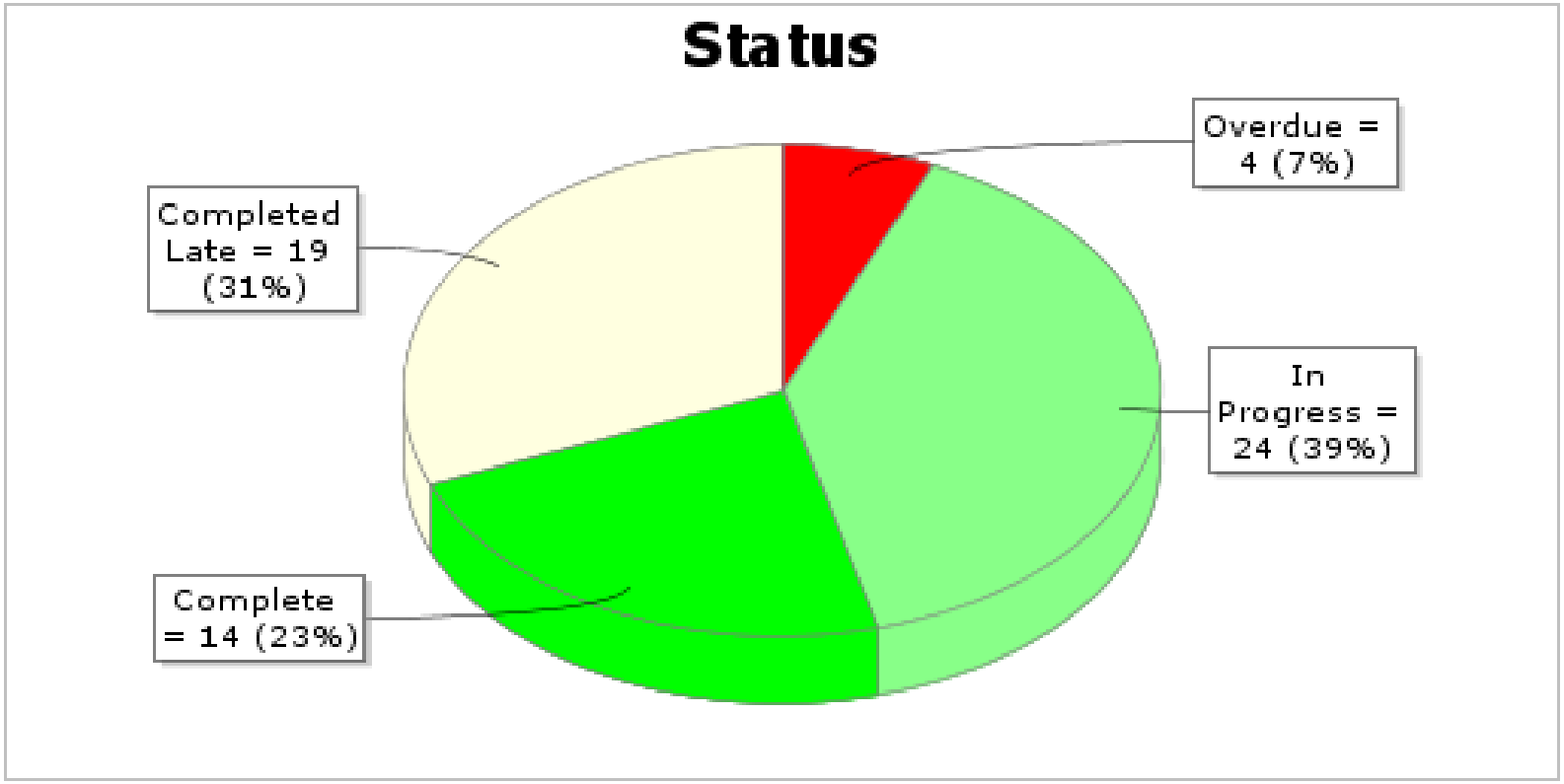
Audit Assignment	Audit Opinion	No. of Audit Actions by Priority	Summary of Audit Findings
Asset Management System	Partial	High = 6 Medium = 4 Low = 0	**1. System Transactions and Records – Leaver access not removed (HIGH)** **Finding:** A sample of five former employees who left between April and November 2020 was examined. Of these five leavers: • Four were listed as current users in RedKite, with all four having Requisition access. • Four leavers were listed on a Redkite system report of users with 'Equipment change location access', meaning they have access to move an asset's location on Redkite. Redkite is not anchored to the Fire Authority's IP address. This means it can be accessed from a personal computer and accessed by leavers listed as active users who no longer have physical access to the Fire Authority's buildings and computers. Discussion with the Asset Management Team and review of Leaver emails also found that removing leavers from the Redkite system is not included on the Leaver checklist listed within the email. **Risk:** If a leaver's access permissions are not removed promptly, there is a risk of unauthorised access to the system, leading to data breaches, manipulating system data and increasing the risk of theft of assets. **2. System Transactions and Records – Resilience in the Asset Management Team (HIGH)** **Finding:** The Asset Management Team established that the Asset and Equipment Manager had been absent for three months. As a result, the Asset Management Technician had picked up the majority of her responsibilities regarding the Asset Management System. Also, telephone calls still had to be made to the absent Manager in certain situations. The Technician stated that he was still learning what she used to do. Many of the processes, other than the Redkite user processes, were found not to be documented. The Manager appeared to be the only staff member trained in carrying out many of these tasks. This demonstrates a resilience issue in the team. **Risk:** If adequate measures are not in place to build resilience and mitigate single points of failure within the team, there is a risk that in the event of a prolonged team absence or a team member leaving the Fire Authority, the Asset Management Team cannot continue business as usual operations. **3. Asset Management Planning, Policies and Procedures – Processes not documented (HIGH)** **Finding:** Many processes were found not to be documented. This included tasks carried out by the Asset Management and Equipment Manager, Asset Management Technician and in the Stores/Mezzanine area that feed into RedKite. It was apparent that there was little awareness between team members and by the Station Commander Research & Development, of what other team members do. Especially of the tasks carried out in the Mezzanine, which are mostly manual and completed outside of Redkite. The team would benefit from mapping the process end to end to better understand their processes and where improvements can be made and help build resilience. **Risk:** If processes are not sufficiently documented there is a risk that staff are unaware of their roles and responsibilities. This could lead to inefficient and inconsistent use of the Asset Management System and reducing the reliability of the data it holds.

Audit Assignment	Audit Opinion	No. of Audit Actions by Priority	Summary of Audit Findings
Asset Management System	Partial	High = 6 Medium = 4 Low = 0	**4. Recording of Assets – Inaccurate record of tests due (HIGH)** **Finding:** During a visit to Beaconsfield Fire Station, it was noted that there was a discrepancy between the number of tests due as seen on the report generated by the Station Commander and those listed for crew users. For example, 87 due tests were listed for the Station Commander for appliance 51P1, but only three listed on the same report viewed by a crew user account. Further discussion with the Station Commander and Asset and Equipment Manager established that the due tests identified are not carried out by fire crews, but by outside contractors and workshops staff and are therefore not visible to operational crews. This indicates that contractor and workshop tests are not always recorded on Redkite. **Risk:** If an accurate list of tests due to be undertaken cannot be viewed by management on Redkite, there is a risk that due tests are not completed, increasing the risk that equipment is obsolete or unsafe. **5. Recording of Assets – Overdue tests (HIGH)** **Finding:** Review of the report of tests due at Beaconsfield Fire Station run from Redkite found that 286 of the 288 tests listed had passed the due date as of 12 November, with one due date listed as being 13 February 2014 and 118 listed as having due dates of 2019 or earlier. A similarly high number of overdue tests were noted for Aylesbury Fire Station as of 3 November 2020. All 179 tests were overdue when viewed against the listed due date. Through discussion with the Station Commander, we were unable to establish whether these tests had been carried out or whether this was a system issue or data quality issue. A sample of 20 assets listed on Redkite was examined to confirm whether equipment tests and inventory checks were carried out promptly and accurately recorded on Redkite. The period covered was from November 2019 to November 2020. Of the 20 assets tested: • In 11 cases, assets were not tested in line with the frequency required by tests loaded onto Redkite. • In four cases, the most recent test was not carried out within a timely manner of the previous test. • In one case, no inventory checks or tests had been carried out since March 2018. In two other cases, an inventory was carried out promptly. However, no tests were carried out on the equipment since 2018 or earlier. In one of these cases, the most recent test was listed as being carried out in October 2014. • One asset was not found during an inventory check. **Risk:** If tests are not carried out periodically and promptly in line with the testing schedule loaded into Redkite for the asset, there is a risk that defective or missing equipment is not detected, increasing the risk that equipment is obsolete or unsafe or that stock levels are not sufficient.

Audit Assignment	Audit Opinion	No. of Audit Actions by Priority	Summary of Audit Findings
Asset Management System	Partial	High = 6 Medium = 4 Low = 0	**6. Recording of Assets – Inaccurate records of stock (HIGH)** **Finding:** A sample of 25 items was selected from the report of current assets generated from Redkite to check whether the assets could be found in the Stores and Workshops area. Of the 25 assets: • Sixteen assets could not be found. In one of these 16 cases, the asset had a system-assigned equipment number but no barcode number or serial number, which are the numbers used by the Authority to identify assets uniquely. If the asset was present in Stores, there would be no unique identifier in Redkite to identify the asset. Values were listed for six of the 16 items that were not located. The highest of these was £345. The total value of items not found for which the value was listed was £687.69. A further sample of 25 items was selected at random from the Stores area to check whether the assets could be identified on the Asset Management System. Of the 25 assets selected: • Seven did not have a label or tag with the barcode number. Of the seven that were not marked or labelled, three had a serial number. However, the serial number could not be found in Redkite. • In the 18 cases where the asset had a barcode label, nine assets could not be identified on Redkite. • In the nine cases where the asset was identified on Redkite, one asset was found in Stores. However, it was listed on the system as being in Stokenchurch. Further testing was carried at Beaconsfield Fire Station. A sample of ten assets was selected from the report of current assets listed on Redkite. Of the ten assets selected: • Two assets were not found at the fire station. One of these assets was a battery for a handheld radio. Discussion with the Station Commander established that these are always listed as auxiliary equipment linked to the station and are not scanned when moved to an appliance or someone takes it with them. However, during the audit visit, the fire crews searched the station appliances (vehicles) for the asset, and it could not be found. • Of the eight assets found, one was not marked with a barcode label, tag or number. **Risk:** If a complete and accurate record of assets and their location is not held on the Asset Management System, there is a risk that the value of the assets on the accounts will be misstated and that assets are not readily available to meet service requirements. **7. System Transactions and Records – Redkite system recovery time (MEDIUM)** **Finding:** Review of the contract with Redkite for the Asset Management System provision found that system recovery arrangements were detailed within the contract. However, the contract does not include an agreed time frame or KPI for the system to be reinstated in the event of system failure. **Risk:** If a system recovery time is not agreed with the Asset Management System provider, there is a risk that in the event of a system outage, the system is not recovered promptly, leading to an inability to continue business as usual operations.

Audit Assignment	Audit Opinion	No. of Audit Actions by Priority	Summary of Audit Findings
Asset Management System	Partial	High = 6 Medium = 4 Low = 0	**8. System Transactions and Records – Assurance of back-ups (MEDIUM)** **Finding:** The RedKite website's review found that the 'Free Hosting' service offered as part of the Asset Management System includes incremental daily back-ups with a full back-up carried out every Tuesday. Whilst reference is not made in the contract to this free hosting service and what it includes, the annual hosting, licence, support, and maintenance fee is specified as a deliverable. However, the Authority does not receive assurance from Redkite that back-ups are taking place in line with the frequency stated. **Risk:** If the Fire Authority is not provided with the assurance that back-ups occur, there is a risk that system data is not backed up in line with the terms of the agreement, leading to data loss in the event of a system outage. **9. System Transactions and Records – Scanners no longer supported (MEDIUM)** **Finding:** Through a walkthrough of the handheld scanner process with fire crews, it was noted that a security alert appears every time the scanner is switched on. The alert states that the security certificate has expired or is not yet valid. Further discussion with the Station Commander and Asset Management Technician noted that Microsoft no longer supports the operating system's version on the scanners. This presents a vulnerability to external attacks wishing to access the system's data. **Risk:** If software is not supported and the security certificate is not valid, there is a risk that control measures to mitigate cybersecurity risks are not sufficient, leading to potential data breaches and a loss of data. **10. Management Information – Stock checks (MEDIUM)** **Finding:** An independent annual stock check, including stock not held centrally, should be carried out by someone from outside of the Asset Management Team and recorded on the Asset Management System. This will assist in assuring senior management over the accuracy of the information held in the Asset Management System and stock levels. Additionally, regular stock checks should be carried out by the Asset Management Team and reconciled to system records to identify any anomalies and reduce the risk of loss. Review of stock checks recorded on Redkite found that the most recent stock check was the Mezzanine Stock Take 2018/19 completed on 1 April 2019. No stock checks were recorded on RedKite for 2020/21 as of November 2020. Discussion with the Asset Management Team and review of Redkite found that the annual independent stock check was due to be carried out in March 2020. However, as a result of the Government's measures to combat Covid-19, this was cancelled, and no new date was set. The most recent independent stock check recorded in RedKite was completed on 1 April 2019. **Risk:** If periodic stock checks are not completed and recorded on Redkite, there is a risk that inaccuracies in the information recorded on Redkite are not detected, and low stock levels of critical assets are not identified, increasing the risk of theft and financial loss. Where independent stock checks are not carried out on an annual basis, there is an additional risk that senior management does not receive adequate assurance over stock levels and the accuracy of the information held in the Asset Management System.

Appendix 2: Current Status of Audit Actions as at 14 June 2021



** 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
Fleet Management (1a & b) Tranman Review	**Medium Priority**	31-Aug-2017	**Finding** 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. **Risk** Where training is not provided on a periodic basis, staff may adopted inappropriate, ineffective, and / or out dated working practices. **Action** 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).	Update from Jez Finden, Fleet Manager: There have been delays due to COVID, leave and the Christmas break, but we are now in the final stages of implementation – we are working through issues identified during UAT and expect to 'go-live' towards the end of this month (Feb).
BMKFA 1718 1830 Property Management (1) Red Kite Functionality	**Low Priority**	31-Mar-2020	**Finding** 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. **Risk** 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. **Action** 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.	Update from Gordon Wylie, Property Manager: Nothing has been started due to pandemic and national lockdown. This is a very low priority.

Title	Priority	Due Date	Description	Latest Note
BMKFA 1819 1947 Project Management BLH (2) The Hub Performance	**Medium Priority**	31-Oct-2019	**Finding** 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. **Risk** 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. **Action** 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.	Update from Mark Hemming, Director of Finance and Assets: The final account still hasn't been settled, and until it is, we are unable to proceed further with any potential claim.

Title	Priority	Due Date	Description	Latest Note
BMKFA 1819 1948 Stores (2) Asset Review	**High Priority**	31-Dec-2019	**Finding** 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. **Risk** 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. **Action** 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.	Follow-up as part of the Asset Management System audit found that this action was not implemented. The action is going to be followed up as part of the 21/22 process mapping work being undertaken by Internal Audit.

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:-