Buckinghamshire & Milton Keynes Fire Authority

MEETING	Overview and Audit Committee
DATE OF MEETING	17 March 2021
OFFICER	Mark Hemming – Director of Finance and Assets Maggie Gibb – Internal Audit Manager
LEAD MEMBER	Councillor David Carroll
SUBJECT OF THE REPORT	**Internal Audit Report: Final Audit Reports**
EXECUTIVE SUMMARY	The purpose of this paper is to update Members on the findings of the finalised Internal Audit reports issued since the last Overview and Audit Committee meeting. The following 2020/21 audits have been finalised: Core Financial Controls (Substantial Opinion), GDPR (Partial Opinion), Asset Management System (Partial Opinion) and Resources Management Application Audit (Partial Opinion).
ACTION	Noting.
RECOMMENDATIONS	That the recommendations raised in the finalised Internal Audit report be noted.
RISK MANAGEMENT	There are no risk implications arising from this report.
FINANCIAL IMPLICATIONS	The audit work is contained within the 2020/21 budget.
LEGAL IMPLICATIONS	There are no legal implications arising from this report.
CONSISTENCY WITH THE PRINCIPLES OF THE DUTY TO COLLABORATE	Not applicable
HEALTH AND SAFETY	There are no health and safety implications arising from this report.
EQUALITY AND DIVERSITY	There are no equality and diversity implications arising from this report.
USE OF RESOURCES	**Communication and progress monitoring;** All audits, follow up reports and further updates will be submitted to the Strategic Management Board and the

	Overview and Audit Committee.
PROVENANCE SECTION & BACKGROUND PAPERS	Internal Audit Plans 2020/21 Internal Audit reports taken to Overview and Audit Committee.
APPENDICES	Appendix A – Core Financial Controls Audit Report Appendix B – GDPR Audit Report Appendix C – Asset Management System Audit Report Appendix D – Resource Management Application Audit Report
TIME REQUIRED	15 minutes.
REPORT ORIGINATOR AND CONTACT	Maggie Gibb – Internal Audit Manager Maggie.Gibb@buckinghamshire.gov.uk 01296 387327

APPENDIX A

Business Assurance and Risk Management

BMKFA Core Financial Controls Audit Report - FINAL (Ref-21/15)

Auditors

Maggie Gibb, Head of Business Assurance (and Chief Internal Auditor)

Selina Harlock, Audit Manager

Alex Prestridge, Senior Auditor

Gillian Kendall, Senior Auditor

CONTENTS

Management Summary

Introduction

The audit of Core Financial Controls was undertaken as part of the 2020/21 Internal Audit plan, agreed by the Overview and Audit Committee. The audit was undertaken during quarter three of 2020/21.

The Core Financial Controls Audit reviewed the Fire Authority's key financial processes including; Creditors, Debtors, Payroll, General Ledger, Grant Income, Banking, VAT and Treasury Management processes. It is vital to the achievement of the Fire Authority's strategic objectives to ensure that there are robust controls in place to enable good financial governance.

Audit Objective

Internal Audit's objectives for this audit were to provide an evaluation of, and an opinion on, the adequacy and effectiveness of the system of internal controls in place to manage and mitigate financial and non-financial risks to the system.

This serves as a contribution towards the overall opinion on the system of internal control that the Chief Internal Auditor is required to provide annually. It also provides assurance to the Section 112 Officer that financial affairs are being properly administered.

Scope of work

The audit activity focussed on the following key risk areas identified in the processes relating to Core Financial Controls:

- Financial Control Framework
- Creditors
- Debtors
- Payroll
- General Ledger
- Grant Income
- Capital
- Banking and Reconciliations
- VAT
- Treasury Management

The audit considered the controls in place at the time of the audit only. Where appropriate, testing was undertaken using samples of transactions since the beginning of the current financial year.

Table 1: Overall Conclusion

Overall conclusion on the system of internal control being maintained	**Substantial**

RISK AREAS	AREA CONCLUSION	No. of High Priority Management Actions	No. of Medium Priority Management Actions	No. of Low Priority Management Actions
Financial Control Framework	Substantial	0	0	0
Creditors	Reasonable	0	0	1
Debtors	Substantial	0	0	0
Payroll	Reasonable	0	2	0
General Ledger	Substantial	0	0	0
Grant Income	Substantial	0	0	0
Capital	Substantial	0	0	0
Banking and Reconciliations	Substantial	0	0	0
VAT	Substantial	0	0	0
Treasury Management	Substantial	0	0	0
		0	2	1

Appendix 1 provides a definition of the grading for each of the conclusions given.

Financial Control Framework

The Financial Regulations were updated in September 2019, reflecting changes to the finance system and current procurement limits. The Regulations detail requirements for all Fire Authority financial systems. These have been published, and the latest approved copies are available to staff on the Intranet.

The Financial Instructions were updated and approved in January 2018 and are available to staff on the BMKFA Intranet. They contain instructions for the effective operation of all financial systems within the Authority and have been reviewed and updated to reflect changes to the Finance system.

Contract Standing Orders (CSOs) were reviewed by Internal Audit. These were updated in February 2020 and include a hyperlink to OJEU limits, ensuring these remain up to date. As the UK has now exited the European Union, the OJEU is replaced by a UK equivalent; Find a Tender Service (FTS).

Another change to public procurement involves transferring the EU Commissions supervisory function to UK Cabinet Office. The UK Cabinet Office will now issue future changes to financial thresholds and public procurement procedures. There is no requirement to update the CSO presently with no change to the current financial thresholds and procurement regulations. The Cabinet Office has started reviewing public procurement regulations with a Green Paper expected in early 2021. As such, the CSO will be reviewed following the Green Paper.

For all key financial processes, process notes were reviewed, confirming that they are up to date. A review of system users found that access to Integra (the Finance system), iTrent (the Payroll system) and Lloyds Link (the Banking system) is appropriately controlled. There is adequate separation of duties required for transactions made within the systems.

Creditors

The Financial Instructions contain guidance on ordering, authorising, and receiving goods and services. The Financial Instructions reference the Financial Regulations and include regulations on the separation of duties, procurement, and expenditure.

A list of users with access to Integra detailing the amounts they can authorise and tasks they can perform was obtained from Finance. Examination confirmed that all users have appropriate access according to their job role. Requests to amend approvers/Budget Holders are sent to Finance to action, with controls in place to ensure that adequate separation of duties is maintained.

Also, there are controls in place to ensure that user roles are not left vacant on Integra when employees leave or transfer. There have been no requests to change approval levels during the 2020/21 financial year.

Budget Holder and Requisitioner roles can enter and authorise purchase orders (POs) via workflow. System parameters on Integra force for a separation of duties, meaning Integra does not allow the same user to raise and authorise a PO. When a PO is created, it workflows to the Budget Holder to approve. Depending on the amount, it is authorised by a senior member of the team (i.e. Director of Finance or Head of Service Development) in line with delegated approval limits. Integra does not allow staff to approve higher than their assigned limit.

However, it was noted that one staff member appearing on the list of approvers had left the Authority in June 2020. Management agrees that although the risk of a leaver accessing the system is low due to physical access being restricted, user access should be terminated in a timely manner as all inactive accounts pose a security risk and are susceptible to hacking.

Examination of a sample of 25 supplier invoices received between April and December 2020 found that:

- In all 25 cases, the invoice was authorised in line with delegations. All demonstrated adequate segregation of duties.
- In all 25 cases, the authoriser agreed to the Scheme of Delegation.
- In 21 cases, the PO was raised before the invoice date. For four cases the PO was raised after the invoice date, however from a review of these exceptions it was established that the anomalies were due to invoices being issued against incorrect or spent orders, so the invoice was reissued but retained the earlier date.
- In 24 cases, invoices were paid after a Goods Receipt Note had been input in Integra. The Finance Team confirmed that the System does not allow payment before goods receipting. The only exception was an item payable to a critical supplier which was processed as an urgent payment via CHAPS and authorised by the Director of Finance and Assets.
- In all 25 cases, the details on the invoice agreed with those on Integra.
- In all 25 cases, the invoice was paid within 30 days of the invoice date.
- In all 25 cases, the invoice was posted to the correct cost centre and GL codes.

It was be noted that the usual protocol of only paying suppliers close to the due date was not in place for the period 20 March 2020 to 4 September 2020. A decision was taken by Senior Management, in line with Government guidance during the Covid-19 pandemic, to assist suppliers by paying invoices as soon as they were received. This is because many of the suppliers are small commercial organisations and early payment would assist with their cash flow. This was not found to have impacted on the Fire Authority's cash flow.

A sample of five credit notes received between April and December 2020 was selected from the Purchase Ledger Transactions Report.

Examination established that:

- For all five credit notes reviewed, the refunds were allocated to the correct supplier.
- In all five cases, the supplier matched that on the original invoice (where received) and PO.

Process notes for creating and amending suppliers were obtained. They detail roles and responsibilities for making changes and carrying out individual checks. The Finance Officer confirmed that changes are made as a result of an email request. If the change involves a change of bank details, the Finance Officer calls the supplier to confirm the changes to bank details.

An email to confirm that the change has been made is then sent to a second Finance Officer for final independent approval, with emails saved on Integra's supplier records.

Examination of a sample of two new vendors and four changes to existing records for the April to November 2020 period found that:

- In both cases where a new vendor was set-up, the reason for the new supplier was not recorded. Discussion with the Principal Accountant and Procurement Manager established that this is due to the vendor set-up process being completed through an e-form. Once the supplier e-form is approved, the supplier is live, and no other information is recorded. However, if the reasoning was not adequate, the Procurement team would reject the request. We confirmed that Procurement check credit histories, and whether there is a possible supplier of similar goods already set up.
- The four changes tested involved deleting unused suppliers, which was carried out late due to Covid-related tasks' prioritisation. Three suppliers were deleted from the system 22 months after deactivation. The remaining supplier was deleted 15 months after deactivation.

Examination of a sample of five weekly BACS runs for the April to December 2020 period confirmed that:

- The total amount and the number of payments on the BACS submission matched those on the payment projection report in all cases.
- BACS control sheets were completed and signed off to indicate that the checker reviewed and completed all checks on all five BACS payments.
- The checker reviewed the payment projection report for duplicate payments and invoices. No duplicate payments were found.
- Payments over £10,000 were checked for accuracy and signed by Principal Accountant. No BACS processing date errors were noted in any of the five cases.

Examination of control account reconciliations completed from April 2020 to October 2020 confirmed that control accounts are reconciled monthly and were subject to review and approval from an independent officer.

The Financial Instructions include guidelines for the appropriate use of purchasing cards. Also, a Purchasing Card User Guide is in place, outlining the Purchasing Card Holder's responsibilities regarding how to use the purchasing card, reconciling the monthly statements and general usage guidelines.

A list of cardholders, along with their agreed monthly spending limit, was obtained. This list shows that 62 staff hold Purchasing Cards, 45 of whom used them between April and December 2020.

A log of Purchasing Card transactions is maintained on Integra. This includes a description of the purchases made, a record of review and authorisation by the card holder’s line manager and attached receipts. Examination of a sample of 20 Purchasing Card transactions posted on Integra between April and December 2020 found that, in all cases, spending limits were in place.

However, instances arose where insufficient documentation was in place to reclaim VAT on valid purchases. However, the Principal Accountant established that the Fire Authority accepts that these are infrequent and insignificant amounts. Where limits had been breached, appropriate authorisation was viewed. There were no transactions that would indicate purchases for invalid items.

Intern Audit found that one purchasing cardholder had left the authority. Although the card had been cancelled within Integra, it had not been cancelled with the bank. This is noted in the findings concerning data maintenance. However, it was confirmed that physical access to both the card and the system had been denied when the staff member left and that no further spend had taken place.

Debtors

Financial Instructions include guidance for the Accounts Receivable functions. Documented procedures for Debtors processes, and how these are actioned on Integra, were obtained from the Principal Accountant and Finance Officer. They were found to be up to date and available to staff on the shared area. Audit confirmed that that access to set up customers is restricted to Finance Officers.

It was noted that the Authority receives income from a number of sources other than funding. An example of this is from workshops services that include MOTs, vehicle repairs, and the sale of used vehicles. The total value of invoices raised under this General Ledger code between April and December 2020 was £5,363.Finance raises invoices for workshops following receipt of an invoice request and proof of sale receipt from the workshop.

Another source of income for The Authority's is from Seconded Officers. A total of £66,390 worth of invoices was raised between April and December 2020. Finance raises Seconded Officer's invoices following receipt of a purchase order from the customer.

Examination of a sample of 18 debtor invoices raised on Integra between April and December 2020 found:

- In all 18 cases, the invoice had been booked to an appropriate budget and GL code.
- Where POs would be expected, these were viewed, and details agreed to the corresponding invoice.
- In all 18 cases, invoices were confirmed as having been input by Finance staff with adequate separation of duties.
- In eight cases, the invoice was paid within 14 days. In nine cases the invoice had not been paid within 14 days, although four had evidence of chasing.
- For the remaining five invoices not paid within 14 days, in one case we found that a payment was made 205 days after the invoice date. We confirmed that Finance chased the payment. Evidence was received from the customer to show that they were in severe financial difficulty, prompting an agreement that the customer would pay when they could. Two invoices had a discrepancy with the dates and no evidence of chasing. Two invoices had payments made 20 and 24 days after the invoice.

Discussions with the Principal Accountant established that the Authority decided to assist private customers with cash flow by not chasing for payment and showing leniency with credit control in line with Government guidance during the Covid-19 pandemic. All debts have now been confirmed as having been paid in full.

A report of Credit Notes was run from Integra listing four credit notes raised between April and December 2020. We selected a sample of two and found that:

- In both cases, the credit note was raised against the correct customer account and budget code.

- One credit note was raised in error, and a matching invoice was raised to cancel it three days later.
- In the remaining case, the credit note was raised four months after the invoice; as the Finance Team the company had gone into administration and no services had been rendered, therefore the credit note cancelled the invoice.

The Debt Management Control Data file includes a summary of outstanding debts, invoice amounts; and provides measurements against Debtors KPIs. The reconciliation and recording of control data are completed monthly. As of October 2020, there was a total of £17,292 outstanding debt owed to the Authority, of which £14,822 was over 60 days old. By November this was £75,778 with the total over 60 days at £12,372. The Principal Accountant confirmed that the increased debt is mainly down to the invoicing profile. It was confirmed that there were no write-offs for 2020/21.

Individual debts that were either shown as paid late or outstanding as of 20 November 2020 were investigated. From a sample review of 10 debts, three had not been chased following the policy, but this was with Senior Management agreement as the customers were in financial difficulty due to Covid-19. Seven were paid more than 30 days late, and of these, three were over 90 days late.

Payroll

Payroll information is processed through the iTrent system. The Fire Service Rota (FSR) planning and scheduling system was fully implemented in April 2020 and is used to record all Watch-based inputs formerly recorded on FB22 forms.

Examination of a sample of 10 starters for the April to November 2020 period confirmed that:

- In all cases, the payroll details were correctly entered on iTrent with a separation of duties. The appropriate authorisations were obtained.
- In one case, where a senior management member returned from retirement, a Succession Planning report was reviewed at a full Fire Authority meeting. A re-engagement letter was sent from the Chief Fire Officer. While this was outside of the normal process, adequate approvals were obtained, which was found to be appropriate for the case.

A sample of 10 permanent changes made between April and November 2020 found that an authorised Change Control Form or an email trail with the appropriate approvals was held on file in nine cases. In one case, authorisation was not held on file for the change. This case involved the addition of CPD payments for an employee. The Payroll and Benefits Manager confirmed that CPD is an allowance requested by the employee and immediate line manager at the annual appraisal. The request is based on evidence of attention to continuous professional development. As well as via the Change Control Form and emails from line managers, a request to pay CPD can also come from HR & OD via email. Discussion established that in these cases, evidence of line manager approval is often not held on file.

Examination of a sample of ten deductions made between April and November 2020 found the following:

- In eight cases, the employee authorised the deduction either through a signed form, email or within the signed employment contract. In two cases, there was no evidence on file that the employee authorised the deduction. Both cases were Prize Draw deductions for which a finding was raised in the 2019/20 Core Financials audit. The Payroll and Benefits Manager established that a review of Prize Draw deductions was planned for March 2021, to re-obtain approval for the Prize Draw deduction.

- In six cases the payslip deduction amount matched the agreed deduction amount. In two cases, the payslip and agreed deduction did not match. Both cases were Prize Draw deductions for which the amount was uplifted since the employees originally signed the forms. Also consistent with Finding 3 from the 2019/20 Core Financial Controls audit.

The Payroll & Benefits Assistant found that whilst up to date Expenses procedures were obtained. They were in the process of being updated at the time of the audit. Examination of a sample of 20 expenses and mileage payments made to staff between April and November 2020 found no exceptions.

All Watch-based overtime is processed into FSR by a Supervisory Manager and noted as a time claim (TOIL) or a pay claim. All items marked as a pay claim are turned out for payment via the running of a monthly pay extract within FSR. The FSR pay process is managed by a series of checks documented on the FSR Payroll Process Checklist. The processes are separated for action between the Payroll Team members. All actions are subject to a secondary peer review before the data is uploaded into iTrent.

Examination of a sample of ten On-Call and Overtime payments made to staff between April and November 2020 found:

- In four cases, an online ESS claim form was completed by the employee on iTrent in line with those employees' process.
- In four cases, the Supervisory Manager processed an FSR claim on behalf of a Watch-based firefighter.
- In one case, an on-call event pay sheet was submitted to Payroll by the employee following attendance of a Safe to Ride course.
- In one case, a request was submitted via email. This was due to a discrepancy with a role, and Terms and Conditions change for the employee. Contractual changes were not communicated effectively to all of the relevant managers. This resulted in an overpayment of £127. We confirmed that corrective action was taken by the employee's line manager and Payroll and that the overpayment was recovered over a period of 90 days through deductions from the employee's pay.
- In all ten cases, the overtime claim was authorised by the employee's line manager.
- In seven cases, the overtime amount on the payslip matched the claim approved by the line manager.
- In all ten cases, the overtime payment was paid in the month of the claim.
- In eight cases, the overtime claimed for was in line with the employment contract. In one case, it was a temporary input approved by the line manager. In one case, the overtime was claimed incorrectly due to a change of role that was incorrectly communicated

A walkthrough of FSR data processing as part of the monthly pay run was undertaken with the Payroll and Benefits Manager. The processing files were obtained for September and October 2020. FSR processing checklists were also obtained for these two months, confirming that they have been completed and that a second officer has checked the inputs.

Examination of a sample of 10 leavers between April and November 2020 found four instances in which a leaver notification was received 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. This means that Payroll is more reliant on manual intervention and affects their timeliness in reporting to HMRC. These process changes were flagged by Payroll as giving rise to additional risk.

General Ledger

Staff are allocated to a 'role' on Integra to ensure adequate separation of duties within the financial processes. Staff cannot access transactions that are not appropriate for their role, for example, setting up new cost centres or cost codes.

Examination of a sample of 14 journals raised over the April to December 2020 period found that:

- In all 14 cases, journals were raised with adequate segregation of duties.
- All journals were found to agree to back documentation.

Review of the two Suspense Accounts (one for payroll errors and a general-purpose account) confirmed that they are reviewed monthly as part of the Control Account reconciliation process. The difference of £704.13 on the payroll suspense was promptly resolved, prior to be being signed off by the Principal Accountant. Requests to amend or add cost centres were confirmed as being carried out in line with a documented process, with a clear audit trail and appropriate authorisation.

Grant Income

We reviewed schedules of expected grant income for 2020/21 provided to the Fire Authority by the authorities and Government departments awarding them. We obtained a letter from the Director of Finance of Assets to the Buckinghamshire Council Service Director of Finance agreeing on the total Fire Authority precept as £14,901,742.82, including 2019/20 surplus.

The letter also states that the precept must be paid to the Fire Authority in twelve equal instalments following the schedule agreed. However, review of email communication between the two authorities established that the Council provided no schedule. Also, payments were due to be made in line with the MHCLG schedule, but these were not. Not having a schedule meant that the Fire Authority had to estimate when they would receive the funding based on the previous year's schedule, reducing the accuracy of cash flow forecasts.

Expected grants for 2020/21 were Fire Revenue New Dimension, Fire Revenue Fire link, BRRS (Business Rates Relief Reimbursement), RSG (Revenue Support Grant), Fire Pensions Grant, Building Risk Review Grant and the agreed 2020/21 Council Tax Precept from both Buckinghamshire Council and Milton Keynes Council.

Examination of a sample of five expected grant payments found the following:

- In four cases, the income expected was received on the expected date. For a BC Council Tax Precept payment, the MHCLG schedule indicated that the payment should be received on 17 September 2020. However, the payment was received on 11 September 2020.
- In four cases, the amount received as shown on the bank statement and Integra agrees with the schedule. In one case, the amount received was £204,138 but the grant amount for the quarter (based on a total payment of £816,565.87 for the year) was calculated as being £204,141. Further discussion and review of cash flow forecasts for 2020-21, found that this was due to be balanced with a larger payment of £204,142.87 expected in Quarter 4.
- In all five cases, there were no conditions listed in the Grant Determination Letter/agreement that applied to BMKFA.
- The grant income was allocated to the correct cost centre/GL account on Integra in all five cases.

Review of Covid Grant Allocations (tranches 1 to 4) confirmed that Fire Authorities' payments were received for the first two tranches. Both payments were received in the bank account on the expected date and as per the expected amount. They were also coded correctly in Integra.

Capital

The Capital Programme for 2019/20 to 2022/23 was approved as part of the MTFP at the Executive Committee meeting on 5 February 2020.

The Principal Accountant confirmed that there were four capital growth bids submitted for 2021-22 budgets onwards. Three of these bids were submitted for a continuation of previous capital bids. Members had provisionally approved these three capital bids as of the audit. However, discussion established that their inclusion in the 2021-22 budget depends on the Fire Authority's funding position in February 2021.

The remaining bid was a new bid and was presented at second officer challenge on 17 December 2020. It is to be updated and to be presented at the second Member challenge in January 2021.

Assets are valued annually by Bruton Knowles. A copy of the valuation report produced in March 2020 was obtained. Five land and building assets were selected from the valuation report and searched for in the asset register. Of these five sites, the up to date valuation was included in the Asset Register in all five cases.

Disposals for 2019/20 totalled £528,063, as per the Asset Register. This included £286,829 of Red Fleet disposals, £134,463 of White Fleet disposals and £106,771 of plant and equipment disposals. There was no recorded land or building disposals for 2019/20. Testing of disposals approved for April to November 2020 was carried out as part of the Asset Management Systems Audit which was undertaken in quarter three.

Banking and Reconciliations

Bank reconciliations are undertaken monthly, and a report is run from Integra which lists any discrepancies. Review of the Control Accounts Reconciliation spreadsheet confirmed that the Bank Control Account Reconciliations are reviewed and signed off by the Principal Accountant monthly.

Access to the bank account via Lloyds Link is restricted to the Director of Finance and Assets, Principal Accountants, and key finance staff members. Levels of access differ depending on staff members' roles, with users requesting a system's role. The Principal Accountant authorises requests. Bank statements are produced from Lloyds Link and entries are matched to creditor and debtor transactions on Integra.

The Finance Officer confirmed that transactions are manually matched as part of the reconciliation process. Bank statements are exported and uploaded into Integra and receipts, and payments are lodged weekly.

We selected a sample of five payments on Lloyds Link bank statements for April, August, June, October, and September 2020. In all five cases, we found that the creditor and payment amount matched that listed on Integra.

Also, we selected a sample of five income transactions recorded on Lloyds Link bank statements. We found that the bank statement was exported and uploaded correctly into Integra; receipts were lodged against the appropriate debtor on both the bank statement and Integra; receipts on the bank statement match those on Integra; and receipts have posted against the bank control account.

VAT

The process for completing the VAT return is now fully automated following the implementation of a new process in September 2019, with process notes updated to reflect this. Following the start of the 2020/21 tax year, the reconciliation is now completed and authorised within Integra and then fed into the HMRC system for submission.

Three VAT returns were reviewed and were seen to agree to back documentation and authorised, reviewed and submitted by the Principal Accountant.

Treasury Management

The Treasury Management Strategy for 2020/21 was approved at the Fire Authority meeting on 12 February 2020. The Strategy refers to CIPFA best practice and guidance on prudential investments and MHCLG guidance. The minimum acceptable credit quality of counterparties for inclusion on the lending list is defined as per CIPFA guidelines for Police and Fire Authorities.

There are Treasury Management Practices as defined in the CIPFA Treasury Management Code of Practice. These were approved at Overview and Audit (O&A) Committee 14 November 2018 and detail the Treasury Management governance within the Fire Authority. Treasury Management reports are produced

quarterly and presented to the O&A Committee. For 2020/21 Quarter 2, the report shows that the accrued interest earned for the first half of 2020/21 was £111k, which is £36k higher than the budget for the period.

A report was obtained of deals executed between April and November 2020 from 'Treasury Live'. It shows all investment deals made, matured investment deals and moving in money market funds from 1 April to 20 November 2020. Over this period there were 23 fixed deals, 13 MMF deals and 11 Call deals. A sample of five investments was reviewed and found that daily cash flow statements were produced for each day in the sample. We also confirmed that all the sample investments had been authorised. They were on the approved counterparty list and within the time limit for investments.

Table 2: Detailed Audit Findings and Management Action Plan

Finding 1: Payroll – Authorisation of CPD payments	Risk Rating	Agreed Management Actions
CPD is an allowance requested for payment at the annual appraisal process by the employee and immediate Line Manager based on evidence of attention to continuous professional development. As with all permanent changes made to payroll, authorisation should be held on file. 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. 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.	**M**	**Action:** Following the discussion of findings during the audit, Station Commanders are now copied in at the point of processing for the addition of CPD payments. **Officer responsible:** Payroll and Benefits Manager **Date to be implemented by:** Immediately

Finding 2: Payroll – Flow of information from HR to Payroll during Leaver and Change of Role processes	Risk Rating	Agreed Management Actions
Following a leaver's notification receipt, HR enter leaver data on iTrent, with a Leaver notification email then sent to the Payroll mailbox. This process should be completed swiftly and before the Payroll cut-off date to ensure that recurring payments to the leaver are promptly removed. 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. 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.	**M**	**Action:** End to end process mapping will be undertaken across HR, Payroll and the Resource Management Team in order to identify areas where processes can be streamlined, and all control weaknesses can be addressed. **Officer responsible:** Payroll and Benefits Manager Head of Human Resources **Date to be implemented by:** December 2021
Finding 3: Creditors - Timely removal of Finance system access	**Risk**	**Agreed Management Actions**

	Rating	
When a member of staff leaves the Fire Authority's employment, or moves to a role that does not require access to a purchasing card (P-Card) or access to the Finance system, access to the card or system should be removed in a timely manner by Finance as part of the leaver/ transfer process. 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. 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.	**L**	**Action:** Six monthly finance system maintenance reviews will be undertaken, which will include a review of system users, their roles and permissions, purchasing card users, supplier and customer maintenance. There were no further purchases using the p-card and this has now been deactivated. **Officer responsible:** Principal Accountant (Technical) **Date to be implemented by:** April 2021

Table 3: Detailed Follow-Up of 2019/20 Findings and Management Action Plan

Report Ref No. 1	Title: Creditors – Purchase Orders	Priority of finding: L	Status: Partially Implemented
Original Audit Finding		**Management Comments & Action Plan**	
Purchasing should be carried out in accordance with Financial Instructions and Financial Regulations. 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.		A reminder will be sent to all suppliers regarding our policy of no purchase order, no payment and a training refresh will be carried out for all relevant BFRS employees to remind all requisitioners/budget holders that a PO needs to be raised prior to an order being placed.	
Follow Up Evaluation		**Management Comments & Action Plan**	
There is a control in place within the Finance system that requires a PO to be in place to pay an invoice. Examination of a sample of 25 invoices received between April to December 2020 found that four POs were raised retrospectively, following receipt of the invoices to which they related. Reasons include instances where suppliers reference POs that have been fully utilised, leading to new POs being raised with the invoice retaining the original date. Also, instances where documents need amendment and instances where invoices are sent to individuals rather than the dedicated creditors' email. If purchase orders are raised retrospectively, there is a risk that inappropriate purchases may be made. Financial commitments could be made outside of the Integra system.		Management will resend an email to all suppliers enforcing the No PO No Pay policy, directing suppliers to send all invoices directly to creditors@bucksfire.gov.uk. An email update will be provided to all Integra users enforcing their responsibilities and the authority's processes. **Officer responsible:** Principal Accountant (Technical)	

Report Ref No. 2	Title: Debtors – Reason for raising Credit Notes	Priority of finding: L	Status: Implemented
Original Audit Finding		**Management Comments & Action Plan**	
Credit notes are raised against the customer account and with the same details included on the original invoice. A valid reason should be given for raising the credit note. 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.		The Principal Accountant will review the credit note explanations as part of the debt management control reconciliations and if these are inadequate, the inputter will be notified to update the system accordingly.	
Follow Up Evaluation		**Management Comments & Action Plan**	
A review of a credit notes report found that there were four credit notes raised between April and December 2020. Examination of a sample of two credit notes found that the reason for raising the credit notes was clear and appeared valid in both cases. Discussion established that the Principal Accountant would pick up inadequate or unclear reasons for raising a credit note as part of the debt management control reconciliations.		N/A	
Report Ref No. 3	**Title: Payroll – Voluntary deductions**	**Priority of finding: L**	**Status: Partially Implemented**
Original Audit Finding		**Management Comments & Action Plan**	
Employees can opt into voluntary payroll deductions for a range of schemes offered by the Fire Authority. The employee should authorise deductions before being actioned on the Payroll system. Examination of a sample of 20 employees paid in December 2019 found the following exceptions: • 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. • In one case where a charity deduction was recorded on the employee's payslip, there was no charity deduction form held on file.		Prize Draw Deductions: All employees currently participating in the prize drawer will be sent a prize draw deduction form to re-confirm their entrance into the prize draw to ensure a record is kept of all participants. Charity Deductions: From 1st April 2020 we have launched a new Tax Free Payroll Giving scheme via an external benefits provider, therefore all prior charitable deductions were ceased from 31.03.2020 with a request to join the new scheme.	

Follow Up Evaluation	Management Comments & Action Plan
Examination of a sample of ten deductions made from Payroll between April 2020 and November 2020 found the following exceptions: • In two cases, there was no evidence on file that the employee authorised the deduction. Both cases were Prize Draw deductions. • Of the eight cases where there was a record of the employee's authorisation held on file, the payslip and agreed deduction did not match in two cases. Both cases were Prize Draw deductions for which the amount was uplifted since the employees originally signed the forms. Discussion with the Payroll and Benefits Manager established that a review of Prize Draw deductions was planned for March 2021, to re-obtain approval for the Prize Draw deduction. 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.	A review of Prize Draw deductions is due to be undertaken in March 2021 to re-obtain approval for the Prize Draw deduction and to relaunch the deduction for the 2021/22 financial year. **Officer responsible:** Payroll and Benefits Manager **Date to be implemented by:** 1 April 2021

Appendix 1: Definition of Conclusions

Key for the Overall Conclusion:

Below are the definitions for the overall conclusion on the system of internal control being maintained.

Definition		Rating Reason
Substantial	There is a sound system of internal control designed to achieve objectives and minimise risk.	The controls tested are being consistently applied and risks are being effectively managed. Actions are of an advisory nature in context of the systems, operating controls and management of risks. Some medium priority matters may also be present.
Reasonable	There is a good system of internal control in place which should ensure objectives are generally achieved, but some issues have been raised which may result in a degree of risk exposure beyond that which is considered acceptable.	Generally good systems of internal control are found to be in place but there are some areas where controls are not effectively applied and/or not sufficiently developed. Majority of actions are of medium priority but some high priority actions may be present.
Partial	The system of internal control designed to achieve objectives is inadequate. There are an unacceptable number of weaknesses which have been identified and the level of non-compliance and / or weaknesses in the system of internal control puts the system objectives at risk.	There is an inadequate level of internal control in place and/or controls are not being operated effectively and consistently. Actions may include high and medium priority matters to be addressed.
Limited	Fundamental weaknesses have been identified in the system of internal control resulting in the control environment being unacceptably weak and this exposes the system objectives to an unacceptable level of risk.	The internal control is generally weak/does not exist. Significant non-compliance with basic controls which leaves the system open to error and/or abuse. Actions will include high priority matters to be actions. Some medium priority matters may also be present.

Management actions have been agreed to address control weakness identified during the exit meeting and agreement of the draft Internal Audit report. All management actions will be entered onto the Pentana Performance Management System and progress in implementing these actions will be tracked and reported to the Strategic Management Board and the Overview & Audit Committee.

We categorise our management actions according to their level of priority:

Action Priority	Definition
High (H)	Action is considered essential to ensure that the organisation is not exposed to an unacceptable level of risk.
Medium (M)	Action is considered necessary to avoid exposing the organisation to significant risk.
Low (L)	Action is advised to enhance the system of control and avoid any minor risk exposure to the organisation.

Appendix 2: Officers Interviewed

The following staff contributed to the outcome of the audit:

Name:	Title:
Asif Hussain	Deputy Director of Finance and Assets
Marcus Hussey	Principal Accountant (Technical Accounting)
Sharon Elmes	Payroll & Benefits Manager
Raheel Iqbal	Finance Officer
Jessica Bunce	Trainee Accountant
Laura Taylor	Principal Accountant (Management Accounting)
Ronda Smith	Procurement Manager

The Exit Meeting was attended by:

Name:	Title:
Asif Hussain	Deputy Director of Finance and Assets
Marcus Hussey	Principal Accountant
Sharon Elmes	Payroll and Benefits Manager

The auditors are grateful for the cooperation and assistance provided from all the management and staff who were involved in the audit. We would like to take this opportunity to thank them for their participation.

Appendix 3: Distribution List

Draft Report:

Mark Hemming	Director of Finance and Assets
Asif Hussain	Deputy Director of Finance and Assets
Marcus Hussey	Principal Accountant

Final Report as above plus:

Jason Thelwell	Chief Fire Officer
Ernst and Young	External Audit

Audit Control:

Closing Meeting	8 January 2021
Draft Report	2 February 2021
Management Responses	11 February 2021
Final Report	XXXX
Audit File Ref	21-15

Disclaimer

Any matters arising as a result of the audit are only those, which have been identified during the course of the work undertaken and are not necessarily a comprehensive statement of all the weaknesses that exist or all the improvements that could be made.

It is emphasised that the responsibility for the maintenance of a sound system of management control rests with management and that the work performed by Internal Audit Services on the internal control system should not be relied upon to identify all system weaknesses that may exist. However, audit procedures are designed so that any material weaknesses in management control have a reasonable chance of discovery. Effective implementation of management actions is important for the maintenance of a reliable management control system.

Contact Persons

Maggie Gibb, Head of Business Assurance

Phone: 01296 387327

Email: maggie.gibb@buckinghamshire.gov.uk

Selina Harlock, Audit Manager

Phone: 01296 383717

Email: selina.harlock@buckinghamshire.gov.uk

APPENDIX B

Business Assurance and Risk Management

BMKFA GDPR - FINAL (Ref-21/19)

Auditors

Maggie Gibb, Head of Business Assurance (and Chief Internal Auditor)

Selina Harlock, Audit Manager

Juan Fosco, Audit Manager

Nav Sidhu, Senior Auditor

CONTENTS

Management Summary

Introduction

The audit of the GDPR was undertaken as part of the 2020/21 Internal Audit plan, agreed by the Overview and Audit Committee. The audit was undertaken during quarter three of 2020/21.

The GDPR audit reviewed the Fire Authority's arrangements for data protection. It is vital to the achievement of the Fire Authority's strategic objectives to ensure that there are robust controls in place to adhere to regulations.

Audit Objective

Internal Audit's objectives for this audit were to provide an evaluation of, and an opinion on, the adequacy and effectiveness of the system of internal controls in place to manage and mitigate financial and non-financial risks to the system.

This serves as a contribution towards the overall opinion on the system of internal control that the Chief Internal Auditor is required to provide annually. It also provides assurance to the Section 112 Officer that financial affairs are being properly administered.

Scope of work

The audit activity focussed on the following key risk areas identified in the processes relating to GDPR:

- Compliance
- Roles and Responsibilities
- Records of Processing Activities (ROPA)
- Third-Party Management
- Retention and Destruction (including Systems and Technology)
- Management Information and Reporting

The audit considered the controls in place at the time of the audit only.

Table 1: Overall Conclusion

Overall conclusion on the system of internal control being maintained	**Partial**

RISK AREAS	AREA CONCLUSION	No. of High Priority Management Actions	No. of Medium Priority Management Actions	No. of Low Priority Management Actions
Compliance	**Reasonable**	**0**	**1**	**1**
Roles and Responsibilities	**Substantial**	**0**	**0**	**0**
Records of Processing Activities	**Reasonable**	**0**	**1**	**0**
Third-Party Management	**Substantial**	**0**	**0**	**0**
Retention and Destruction (including Systems and Technology)	**Reasonable**	**0**	**1**	**0**
Management Information and Reporting	**Partial**	**1**	**0**	**0**
		1	**3**	**1**

Appendix 1 provides a definition of the grading for each of the conclusions given.

Compliance

The Authority has a Data Quality procedure which 'sets out processes to assure that information risks are being addressed adequately so that all data and information that is owned or managed by the Authority is accurate, available to Authority's people when needed, secured appropriately to prevent unauthorised access or alteration, and destroyed when no longer required'. The procedure was approved in January 2018. Discussions with the Information Governance and Compliance Manager confirmed the procedure is to be reviewed by the end of the financial year.

A Record Retention and Disposal/Information Assets Register (IAR) procedure is also in place. Its purpose is to ensure that the Authority holds records following legislation and business needs. This procedure was last reviewed and approved by the Head of Service Development in December 2019.

Other procedures are also in place, such as:

- Dealing with Requests for Information; and
- Redacting Sensitive Information.

However, our review identified that the 'Data Quality', 'Dealing with Requests for Information' and 'Redacting Sensitive Information' procedures referred to an Integrated Impact Assessment, which is no longer in place. It was also identified that the Redacting Sensitive Information procedure did not refer to when it was last reviewed and approved.

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.

Roles and Responsibilities

A Senior Information Risk Owner (SIRO) and a Data Protection Officer (DPO) are defined on the Authority's website. The roles and responsibilities of both are clearly defined in the procedures available to staff.

An Information Management Risk Register is in place which records GDPR risks and the ownership of each risk. Discussions with the DPO (who is the Information Governance and Compliance Manager) confirmed that the register is reviewed monthly to update risks identified within. Review of the Strategic Management Board (SMB) and Monitoring Board agendas confirmed that the review of the register is a standing item for both meetings.

Records of Processing Activities (ROPA)

Following the ICO's Accountability Framework guidance, ROPAs must, as a minimum, include:

- The organisation's name and contact details, whether it is a controller or a processor (and where applicable, the joint controller, their representative and the DPO);

- The purposes of the processing;
- A description of the categories of individuals and personal data;

We confirmed that a central ROPA spreadsheet is in place detailing the various processing activities undertaken. The central ROPA spreadsheet includes evidence of purpose, legal basis, and categories of individuals and information, in line with the ICO's Accountability Framework guidance.

Departments within the Authority are also responsible for retaining their ROPA spreadsheets. The Safeguarding's ROPA was reviewed. It was found that it did not specify whether it was a controller or a processor or the retention schedules.

Third-Party Management

Companies invited to tender are required to complete the Standard Invitation to Tender document, which includes preliminary questions regarding data protection and security. Any interested company has to confirm how it complies with GDPR legislation and should list the key actions undertaken to confirm compliance; it also has to confirm that data is held within the EU/UK. Additionally, standard wording is included in contract terms and conditions regarding confidentiality, data protection and GDPR.

We selected a sample of four contracts. We confirmed that the Standard Invitation to Tender document was completed in full by the companies. The respective contracts in place included the standard confidentiality, data protection and GDPR wording. The contracts reviewed were the following:

- Corporate Website;
- Incident Command Training;
- Fleet Management System; and
- Learning Management System.

Also, an e-form is used by the Procurement team to check compliance before approving to proceed with the tender/procurement process. The e-form includes, among others, a mandatory field to identify if the supplier/contractor processes personal information. If this is identified, the originator is referred to the DPO to seek further advice as to what additional documentation is required before setting up the new supplier/contract, such as a Data Protection Impact Assessment (DPIA). From the sample above, we identified that the Fleet Management System and Learning Management System required a DPIA. Testing confirmed that a DPIA was completed for both of these contracts.

Retention and Destruction (Including systems and Technology)

The Records Retention and Disposal Information Asset Register procedure states that information stewards are responsible for ensuring the timely archiving and/or destruction of records. They are also responsible for advising the information owners where it is believed a retention timescale should be amended following legislation or business needs.

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. For paper documents, which have been archived, an archive master schedule is in place which states the retention period. Archive Centre Ltd manages the archived documents.

However, the Authority relies on information stewards to ensure that electronic data is disposed of (according to the retention schedule) and there is no mechanism in place to ensure this occurs.

The Authority's email system will address each email as it passes inbound or outbound from the servers. The system interrogates the email and attached documents looking for personally identifiable information, including but not limited to, EU Nation Identification numbers, Social Security Numbers or bank details. Once identified, the system generates an incident report passed to the ICT Service Desk for review and challenge users as to why they are sending the information.

Management Information and Reporting

The Business Transformation Board (BTB) terms of reference specify that one of the board's terms of reference is to review risks associated with change and that meetings are held monthly. We confirmed that meetings were held in June, August and September 2020. Also, quarterly Monitoring Board meetings occur where items such as directorate and corporate risks are discussed. Our review of meetings minutes from June to October 2020 confirmed that discussions around risks and GDPR took place and are being monitored.

During the audit fieldwork, the DPO confirmed that there had been no 'reportable breaches' at the Authority. The DPO noted that there had been three 'near misses' at the Authority between April and December 2020. One of which had been reviewed with investigations finalised and the remaining three were ongoing.

Our review of the investigation finalised found that a staff member had been granted inappropriate access to a certain folder. The access has been flagged before any reportable breaches. The report and investigation were documented using email trails.

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 Report 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.

We confirmed that a documented investigation had been undertaken by the DPO raising 12 recommendations. The investigation raised a recommendation requiring HR to identify all employees whose personally identifiable information has been subject to inappropriate access and speak to the relevant Manager, who will be responsible for explaining to these employees that information has been released, measures taken, and those being taken to prevent further occurrences.

Table 2: Detailed Audit Findings and Management Action Plan

Finding 1: Data Incidents and Reporting	Risk Rating	Agreed Management Actions
Any data breaches/incidents at the Authority should be reported to the DPO and recorded in a data breach log along with lessons learned. Awareness should be regularly raised throughout the Authority regarding reporting of data breach incidents and lesson learned should be reported on at board meetings. 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. 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.	**H**	**Action:** The recommendations of the DPO are currently being considered and further investigatory work is being undertaken. Actions will be determined once this work is complete. **Officer responsible:** Director of Finance and Assets **Date to be implemented by:** June 2021
Finding 2: E-learning modules	**Risk Rating**	**Agreed Management Actions**
E-learning modules are on an annual basis with rotation between the e-learning modules of GDPR and Cyber Security. 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.	**M**	**Action:** Follow up with line managers of staff who are required to complete the training but have not done so within the specified time periods to ensure outstanding learning is completed. **Officer responsible:** Information

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.		Governance and Compliance Manager **Date to be implemented by:** June 2021
Finding 3: Records of Processing Activities (ROPAs)	**Risk Rating**	**Agreed Management Actions**
ROPAs across all departments and stations are held in a digital catalogue accessible to the Information Governance and Compliance Manager; the catalogue should be linked to all individual ROPA's held within the Authority. The catalogue is used to complete compliance checks on ROPAs held across the Authority to ensure it meets ICO requirements. 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. 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.	**M**	**Action:** Agreed. ROPAs to be reviewed. **Officer responsible:** Information Governance and Compliance Manager **Date to be implemented by:** September 2021
Finding 4: Retention and Destruction	**Risk Rating**	**Agreed Management Actions**
The Records Retention and Disposal Information Asset Register procedure states that information stewards are responsible for ensuring the timely archiving and/or destruction of records and advising the Information Owners where it is believed a retention timescale should be amended following legislation or business needs. 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. 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.	**M**	**Action:** Agreed. A mechanism to review data disposals inline with the retention schedules will be formalised and monitored. **Officer responsible:** Information Governance and Compliance Manager **Date to be implemented by:** December 2021

Finding 5: Procedures	Risk Rating	Agreed Management Actions
Policies and procedure should be reviewed regularly with revisions and approval dates recorded within each document. 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. 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.	**L**	**Action:** Agreed. Procedures will be reviewed and updated where necessary and review and approval dates updated. **Officer responsible:** Information Governance and Compliance Manager **Date to be implemented by:** March 2022

Appendix 1: Definition of Conclusions

Key for the Overall Conclusion:

Below are the definitions for the overall conclusion on the system of internal control being maintained.

Definition		Rating Reason
Substantial	There is a sound system of internal control designed to achieve objectives and minimise risk.	The controls tested are being consistently applied and risks are being effectively managed. Actions are of an advisory nature in context of the systems, operating controls and management of risks. Some medium priority matters may also be present.
Reasonable	There is a good system of internal control in place which should ensure objectives are generally achieved, but some issues have been raised which may result in a degree of risk exposure beyond that which is considered acceptable.	Generally good systems of internal control are found to be in place but there are some areas where controls are not effectively applied and/or not sufficiently developed. Majority of actions are of medium priority, but some high priority actions may be present.
Partial	The system of internal control designed to achieve objectives is inadequate. There are an unacceptable number of weaknesses which have been identified and the level of non-compliance and / or weaknesses in the system of internal control puts the system objectives at risk.	There is an inadequate level of internal control in place and/or controls are not being operated effectively and consistently. Actions may include high and medium priority matters to be addressed.
Limited	Fundamental weaknesses have been identified in the system of internal control resulting in the control environment being unacceptably weak and this exposes the system objectives to an unacceptable level of risk.	The internal control is generally weak/does not exist. Significant non-compliance with basic controls which leaves the system open to error and/or abuse. Actions will include high priority matters to be actions. Some medium priority matters may also be present.

Management actions have been agreed to address control weakness identified during the exit meeting and agreement of the draft Internal Audit report. All management actions will be entered onto the Pentana Performance Management System and progress in implementing these actions will be tracked and reported to the Strategic Management Board and the Overview & Audit Committee.

We categorise our management actions according to their level of priority:

Action Priority	Definition
High (H)	Action is considered essential to ensure that the organisation is not exposed to an unacceptable level of risk.
Medium (M)	Action is considered necessary to avoid exposing the organisation to significant risk.
Low (L)	Action is advised to enhance the system of control and avoid any minor risk exposure to the organisation.

Appendix 2: Officers Interviewed

The following staff contributed to the outcome of the audit:

Name:	Title:
Gerry Berry	Information Governance and compliance manager
Dave Thexton	ICT Manager
Joanne Cook	Community Safety and Safeguarding Manager
Anne Stunnell	Head of Human Resources
Ronda Smith	Procurement Manager

The Exit Meeting was attended by:

Name:	Title:
Gerry Berry	Information Governance and compliance manager
Dave Thexton	ICT Manager
Joanne Cook	Community Safety and Safeguarding Manager
Anne Stunnell	Head of Human Resources

The auditors are grateful for the cooperation and assistance provided from all the management and staff who were involved in the audit. We would like to take this opportunity to thank them for their participation.

Appendix 3: Distribution List

Draft Report:

Gerry Berry	Information Governance and compliance manager
Dave Thexton	ICT Manager
Joanne Cook	Community Safety and Safeguarding Manager
Anne Stunnell	Head of Human Resources
Mark Hemming	Director of Finance and Assets

Final Report as above plus:

Jason Thelwell	Chief Fire Officer
Ernst and Young	External Audit

Audit Control:

Closing Meeting	16 December 2020
Draft Report	2 February 2021
Management Responses	23 February 2021
Final Report	24 February 2021
Audit File Ref	21-19

Disclaimer

Any matters arising as a result of the audit are only those, which have been identified during the course of the work undertaken and are not necessarily a comprehensive statement of all the weaknesses that exist or all the improvements that could be made.

It is emphasised that the responsibility for the maintenance of a sound system of management control rests with management and that the work performed by Internal Audit Services on the internal control system should not be relied upon to identify all system weaknesses that may exist. However, audit procedures are designed so that any material weaknesses in management control have a reasonable chance of discovery. Effective implementation of management actions is important for the maintenance of a reliable management control system.

Contact Persons

Maggie Gibb, Head of Business Assurance

Phone: 01296 387327

Email: maggie.gibb@buckinghamshire.gov.uk

Selina Harlock, Audit Manager

Phone: 01296 383717

Email: selina.harlock@buckinghamshire.gov.uk

APPENDIX C

Business Assurance and Risk Management

Asset Management System Audit Report - FINAL (Ref-21/10)

Auditors

Maggie Gibb, Head of Business Assurance (and Chief Internal Auditor)

Selina Harlock, Audit Manager

Juan Fosco, Audit Manager

Alex Prestridge, Senior Auditor

CONTENTS

Management Summary

Introduction

The Asset Management System audit was undertaken as part of the 2020/21 Internal Audit plan, agreed by the Overview and Audit Committee. The audit was undertaken during quarter three of 2020/21.

The Asset Management System audit reviewed the Fire Authority's arrangements for the purchase, custody and issue of assets, covering operational equipment and property assets. It is vital to the achievement of the Fire Authority's strategic objectives to ensure that there are robust controls in place, preventing the loss or misuse of assets. It is also essential to ensure that the necessary stock and equipment is held.

Audit Objective

Internal Audit's objectives for this audit were to provide an evaluation of, and an opinion on, the adequacy and effectiveness of the system of internal controls in place to manage and mitigate financial and non-financial risks to the system.

This serves as a contribution towards the overall opinion on the system of internal control that the Chief Internal Auditor is required to provide annually. It also provides assurance to the Section 112 Officer that financial affairs are being properly administered.

Scope of work

The audit activity focussed on the following key risk areas identified in the processes relating to the Asset Management System:

- Asset Management Governance
- System Transactions and Records
- Asset Management Planning, Policies and Procedures
- Management Information
- Recording of Assets
- Asset Base Verification and Reconciliation to Finance System
- Additions
- Disposals

The audit also followed up on the findings of the 2018/19 Stores audit.

The audit considered the controls in place at the time of the audit only. Where appropriate, testing was undertaken using samples of transactions since the beginning of the current financial year.

Table 1: Overall Conclusion

Overall conclusion on the system of internal control being maintained	**Partial**

RISK AREAS	AREA CONCLUSION	No. of High Priority Management Actions	No. of Medium Priority Management Actions	No. of Low Priority Management Actions
Asset Management Governance	**Substantial**	**0**	**0**	**0**
System Transactions and Records	**Partial**	**2**	**3**	**0**
Asset Management Planning, Policies and Procedures	**Partial**	**1**	**0**	**0**
Management Information	**Reasonable**	**0**	**1**	**0**
Recording of Assets	**Limited**	**3**	**0**	**0**
Asset Base Verification and Reconciliation to Finance System	**Substantial**	**0**	**0**	**0**
Additions	**Substantial**	**0**	**0**	**0**
Disposals	**Substantial**	**0**	**0**	**0**
		6	**4**	**0**

Appendix 1 provides a definition of the grading for each of the conclusions given.

Asset Management Governance

The Financial Regulations were last updated in September 2019 and outline the Executive Committee's role in the Asset Management System's governance.

The Financial Regulations include the Terms of Reference of the Executive Committee. Its objectives relating to the role in overseeing the Asset Management System are:

- To consider and determine the annual programme for the replacement of vehicles and other major capital schemes
- Consider and advise the Authority on the financial effects of significant development strategies, plans, major acquisitions, contracts etc.
- To oversee the use of land and property and other significant resources (e.g. information technology, vehicles and communications equipment)

The Financial Regulations also state that: "Directors and second-tier managers should ensure records and assets are properly maintained and securely held in a method approved by the Chief Finance Officer. They should also ensure that contingency plans for the security of assets and continuity of service in the event of disaster or system failure are in place."

The Contract Standing Orders document provides more specific requirements relating to the acquisition and disposal of property and non-property assets.

The Asset Management System's governance was operating in line with the Financial Regulations, Contract Standing Orders and the Fire Authority's Scheme of Delegation.

There is a contract with Redkite for the provision of the Asset Management System. The contract outlines, among others, Redkite's responsibility for hosting the system on secure servers, obligations regarding system security, recovering corrupt files and software upgrades. This contract was signed in April 2019 and is valid until March 2022. We also confirmed that the contract was signed and dated by appropriate representatives of BMKFA and Redkite Systems. A tender process was not carried out as the contract's value is £9,000 per year, under the £10,000 threshold at which a tender process must be completed.

System Transactions and Records

Members of the Asset Management Team and Property Team can add or remove assets on the system. Only the Asset Management Systems Officer and two other Asset Management Team members can create a new user on the system. When adding a new user, the HR department informs the Stores mailbox that user access is required.

Reports of users can be run from RedKite based on individual access levels. An Access Level Report was obtained for users with access level 'Equipment change location access'. Compared to a list of all BMKFA staff, all users on the list were found to have roles that require them to move equipment between locations.

The Asset Management Technician established that Leaver emails are automatically sent by iTrent (the Payroll system) when a Leaver is actioned. Emails are sent to the Stores mailbox, including a checklist of actions to be completed before the employee's leave date. However, our review of the email sent out found that removing leavers from the Redkite system is not included on the checklist.

A report of employees who left the Fire Authority's employment between April and November 2020 was obtained from the Payroll and Benefits Manager. From a sample of five leavers, the following was found:

- All five users were granted appropriate access levels for their job role.
- In one case, the leaver was no longer listed as a user on Redkite. In the remaining four cases, the leavers were still listed as users in Redkite, with all four having Requisition access.
- In one case, the leaver did not appear on a system report of users with 'Equipment change location access'. In the remaining four cases, the leavers were listed on this report, 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 Authority's buildings and computers.

Review of the Redkite website and contract found that sufficient provisions were made for system back-ups as part of the 'Free Hosting' service, with systems and data backed up incrementally every day with a full back-up carried out every Tuesday. The data is retained at two secure sites. Provisions for system recovery are made within the RedKite 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.

Through discussion with the Asset Management Technician and 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 warning states that the security certificate has expired or is not valid. Further discussions noted that Microsoft no longer supports the version of the operating system on the scanners. This presents a vulnerability to external attacks wishing to access the system's data.

Discussion with the Asset Management Team established that, at the time of the audit, the Asset and Equipment Manager had been out of the business for three months. Therefore, the Asset Management Technician picked up the majority of 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 core Redkite processes, were found not to be documented. The Manager appeared to be the only staff member trained in carrying out many of these tasks demonstrating a resilience issue in the team.

A business continuity control was recently implemented which consists of a logbook to manually record breathing apparatus (BA) cylinders and their location. This was following an incident in which there was a contaminated cylinder containing oil and moisture due to a faulty air compressor. This issue was picked up as the result of a spot check but had it not been detected, it could present a risk to a fire-fighter's life. A lessons-learnt document was produced by BMKFA and shared nationally with other Fire Authorities.

Asset Management Planning, Policies and Procedures

The Capital Strategy, Property Strategy and Fleet Strategy were obtained from the Director of Finance & Assets. All three strategies were approved by the Executive Committee, with the Capital Strategy being approved during the audit by the Executive Committee on 18 November 2020. The three strategies include five-year plans covering all assets of significant value.

User guides produced by Redkite are available on the Redkite application. This includes separate user guides for Stores, the Equipment Management System (dated February 2020) and the handheld scanners used as part of the Equipment Management System (dated May 2015). We established that these guides are updated in line with system updates, and all are up to date with regards to current processes.

The Asset Management User Guidance Note dated March 2019 was obtained from the Asset Management and Equipment Manager. It includes a version number and the date approved but does not provide a date for subsequent review, however the guidance was found to be up to date. This addresses the finding from the 2018/19 Stores audit regarding the update of policies and procedures.

Training was also available for Redkite users when it was first rolled out in 2014. Slides for the training are available on the system. However, discussion established that no formal training is provided to new users and instead receive 'cascade training' (on the job training).

While the user guidance obtained was deemed adequate covering user processes with sufficient detail and clarity, there were processes not documented, including tasks carried out by the Asset Management and Equipment Manager, Asset Management Technician, and the Stores/Mezzanine that feed into RedKite.

Through discussions with staff, it was apparent that there was little awareness between team members and the Station Commander Research & Development of what other team members do. Especially of the processes carried out in the Mezzanine regarding storing, identifying, recording and distributing equipment.

Management Information

The Property Manager and Facilities Manager established that KPIs are in place regarding response times for rectifying property defects. Defects are split into three categories: Red (the most urgent - critical to operations), Amber, and Green. These performance indicators are measured and recorded in RedKite. Discussion with the Property and Facilities Manager established that site visits had been reduced to a minimum as a result of measures to control the spread of Covid-19. Contractors had been sent out only in the case of Red defects and for some Amber defects.

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. As a result of Covid, this was cancelled, and no new date was set. The most recent independent stock check recorded in RedKite was completed on 1 April 2019.

Recording of Assets

Assets are tested and inspected periodically in line with a pre-determined schedule to identify any faults or defects and to confirm that the asset is present. Discussion with the Station Commander established that the frequency of tests is dependent on the asset. Details of the test and frequency are provided by

the manufacturer and/or set nationally (usually in the Fire Service Manual). Test schedules and instructions are loaded into Redkite by the Asset Management and Equipment Manager. Regular inventory checks are also carried out by Fire Crews and the Asset Management team. These can be either ad-hoc or as per a schedule loaded onto Redkite.

On 12 November 2020, we visited Beaconsfield Fire Station to conduct walkthroughs of the Duty Watch equipment testing processes. During the visit, 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 as viewed by a crew user account.

Review of the report run from Redkite found that 286 of the 288 tests listed had passed the due date as of 12 November 2020. One due date recorded as 13 February 2014 and 118 listed as having due dates 2019 or earlier.

A similarly high number of overdue tests were noted for Aylesbury Fire Station as of 3 November with all 179 tests outstanding. 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 nine cases, assets were tested in line with the frequency required by tests loaded onto Redkite. In 11 cases, they were not.
- In 16 cases, the most recent test listed on Redkite was promptly carried out considering the previous test date. In four cases, the most recent test was not carried out within a timely manner of the last 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.

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:

- Nine assets were found in the location listed on Redkite. In 16 cases, the asset could not be found. In one of these 16 cases, the asset had no barcode number or serial number. Therefore, this asset may have been present in the Stores area, but there was no unique identifier in Redkite that could be matched to the asset in Stores.
- In all nine cases where the asset was found, it was marked with a barcode label or sticker or engraved with the barcode number.

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 chosen assets:

- In 18 cases, the asset had a label or tag with the barcode number. Seven did not. Three assets had a serial number of the seven that were not marked with a barcode label or tag. However, the serial number was not found recorded in Redkite.

- In the 18 cases where the asset had a barcode label or sticker or was engraved with the asset number, nine were found on Redkite. The remaining nine assets could not be identified on Redkite.
- For the nine assets identified on Redkite, eight had their location correctly recorded on Redkite. However, the remaining asset was found in Stores but was listed on the system as being in Stokenchurch.

Further testing was carried out during a site visit to Beaconsfield Fire Station to determine whether the issues raised above were limited to Stores. A sample of ten assets was selected from Redkite. Of the ten assets selected:

- Eight assets were found at the Fire Station, and two were not found. One of the assets not located was a battery for a handheld radio. Discussion with the Station Commander and Beaconsfield fire crew 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, seven were marked with a barcode label tag or number. One asset was not marked or labelled.

A further sample of 10 items was selected from around the Fire Station to check whether the assets could be identified on the Asset Management System. Of the 10 assets selected:

- All ten assets were marked with a barcode label or tag.
- All ten assets were identified on Redkite as being in the location where they were found.

Stock checks are periodically carried out by both the Asset Management Team and independently. Results should be recorded on Redkite. However, no stock checks were recorded on RedKite for 2020/21 as of November 2020. At the time of the audit, a stock check of radios was being undertaken by the Asset Management Team and recorded manually. However, no record of this stock check could be found on Redkite.

Asset Base Verification and Reconciliation to Finance System

The 2018/19 Stores audit found no assurance that the values maintained on Redkite were the same as those maintained on the General Ledger. A recommendation was raised suggesting that the Asset Management System is interfaced to the General Ledger if possible.

The Trainee Accountant and Principal Accountant established that Redkite could not be interfaced into Integra. All interaction between the two systems has to involve manual processes.

To address this issue, an 'Operational equipment Redkite' cost element was set up on Integra by Finance, along with a query used to run reports of purchase orders raised against this code. A Purchase Order report was also created in Redkite for orders with a PO number. This is run monthly by the Principal Accountant (Management Accounting).

We confirmed that monthly reconciliations are completed by the Trainee Accountant as part of the monthly data upload process and sent to the Principal Accountant (Technical Accounting) for him to check and sign off. This process was deemed to be sufficient.

Additions

A walkthrough of the purchasing and goods receipting process confirmed appropriate segregation of duties when purchasing new stock. The Asset Management and Equipment Manager usually requisition orders. Testing of the ordering process for the Fire Authority as a whole will be completed in detail in the Core Financial Controls audit.

We established that an Asset Valuation is undertaken by Bruton Knowles annually. The most recent report, dated 31 March 2020, was obtained and we confirmed that the previous valuation was completed on 1 April 2019. A full asset register with asset values, including operational equipment, is maintained by the Director of Finance and Assets.

Disposals

In October 2020, 154 operational assets were approved for disposal, consisting of 54 capital assets and 100 assets listed as stock items. These assets were identified by the Station Commander Research & Development and Asset Management Team as being surplus to requirements, with potential buyers for the equipment. This request was subject to adequate check and challenge from Finance, including reviewing these items against the asset register. Asset disposal forms were completed by the requestor and approved by the Director of Finance and Assets in each case. Our testing covered the entire population submitted in the current financial year and found that the appropriate authorisations were received in each case. Land and Buildings considered for disposal are subject to additional review by Fire Authority members.

Table 2: Detailed Audit Findings and Management Action Plan

Finding 1: System Transactions and Records – Leaver access not removed	Risk Rating	Agreed Management Actions
When an employee leaves the Fire Authority's employment, the Asset Management team is notified by way of a Leaver email sent out by HR. The employee's access permissions to all BMKFA systems, including Redkite, should be removed as part of this process. 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. 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.	**H**	**Action:** Changes will be made to Leaver notification information to include removal of Red Kite access. An exercise will be undertaken to assess whether there was any activity for users identified as not having been removed after they left. **Officer responsible:** Station Commander Research & Development **Date to be implemented by:** Immediately

Finding 2: System Transactions and Records – Resilience in the Asset Management Team	Risk Rating	Agreed Management Actions
There should be a sufficient provisions and service resilience within the team to ensure business continuity should a risk event occur. 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. 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.	**H**	**Action:** There are user guides available on the Red Kite software programme and a Red Kite Asset Management user guide on the intranet. These are accessible to all staff. The Asset Management Technician has been made aware of these documents. Access rights have been checked to ensure the suitable persons have access and can download Red Kite user guides from the login screen. Documentation to be reviewed for any gaps and process notes to be updated where required. **Officer responsible:** Asset Management and Equipment Manager Asset Management Technician **Date to be implemented by:** July 2021

Finding 3: Asset Management Planning, Policies and Procedures – Processes not documented	Risk Rating	Agreed Management Actions
Up to date asset management procedures should be in place. The procedures should be compliant with Financial Regulations and Financial Instructions and help deliver the asset management plan. 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. 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.	**H**	**Action:** We have ensured that all staff have access to the relevant user manuals. We will review the roles and responsibilities of the Asset Team and ensure that Manager, deputy and SC R&D are aware of work practices and procedures of the whole team. Create a series of flowcharts showing workflow that could be picked up by "new" staff in the event of staff leaving/prolonged sickness or secondment out of current position. This will be supported by the end-to-end process mapping within the Internal Audit Plan for 2021-22. **Officer responsible:** Station Commander Research & Development Asset Management and Equipment Manager **Date to be implemented by:** September 2021

Finding 4: Recording of Assets – Inaccurate record of tests due	Risk Rating	Agreed Management Actions
Fire crews, workshop staff, and contractors must undertake regular stock checks and tests of equipment at fire stations and on appliances (vehicles). Due tests are listed on handheld devices used to scan asset barcodes and record test completion and results on Redkite. Users and management can also view a list of tests due on a computer. 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. 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.	**H**	**Action:** Review of the testing frequency of equipment listed on Red Kite. Ensure workshops staff are testing, recording, and accessing the required testing information. Set a regular review of outstanding tests for all equipment and who would carry out the test and who would have access to view these records. This will be supported by the end-to-end process mapping within the Internal Audit Plan for 2021-22. **Officer responsible:** Station Commander Research & Development **Date to be implemented by:** September 2021

Finding 5: Recording of Assets – Overdue tests	Risk Rating	Agreed Management Actions
Fire crews must undertake regular stock checks and tests of equipment at fire stations and on appliances (vehicles). The frequency of these tests and inventory checks depends on the individual asset's testing schedule, usually dictated by the PIT number assigned to the asset. Results of tests and inventory checks should be recorded on Redkite by crews using either a handheld scanner or computer. 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. 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.	**H**	**Action:** Review of testing frequencies and recording of all equipment on Red Kite. Additional training for the operational crew in the recording of tests. **Officer responsible:** Station Commander Research & Development **Date to be implemented by:** July 2021

Finding 6: Recording of Assets – Inaccurate records of stock	Risk Rating	Agreed Management Actions
Stock records should enable identification of assets owned and determine those in use or not in use. The location of the asset should also be recorded accurately on the asset management system. 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. Testing of a different sample of ten items selected at random from the Fire Station found no exceptions. All assets could be identified in the Asset Management System.	**H**	**Action:** As part of the stock check of equipment within stores and on mezzanine equipment will be checked to ensure that it has an asset/barcode tag and that this is recorded against the serial number of the equipment item and recorded on Red Kite. **Officer responsible:** Asset Management Technician **Date to be implemented by:** August 2021

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.		
Finding 7: System Transactions and Records – Redkite system recovery time	**Risk Rating**	**Agreed Management Actions**
There should be a provision for timely system recovery to reduce the risk of loss of data or an inability to continue business as usual operations should the system be impacted by a risk event occurring. 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. 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.	**M**	**Action:** A review of the contract will be undertaken to look at the feasibility of adding data recovery options into the contract. Contact Red Kite and determine their Business Continuity plan for protecting Data. **Officer responsible:** Procurement Manager **Date to be implemented by:** September 2021
Finding 8: System Transactions and Records – Assurance of back-ups	**Risk Rating**	**Agreed Management Actions**
Data held on Redkite should be backed up periodically by the system provider. 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. 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.	**M**	**Action:** Contact Redkite to provide evidence and reassurance regarding periodic back-ups **Officer responsible:** Asset and Equipment Manager **Date to be implemented by:** Immediately

Finding 9: System Transactions and Records – Scanners no longer supported	Risk Rating	Agreed Management Actions
Fire crews use handheld scanners to record the results of equipment tests and inventory checks on Redkite. As with the Asset Management System's computer-based version, these should be subject to the necessary system updates. 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. 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.	**M**	**Action:** We have started a review of Red Kite and the equipment associated with Red Kite. We have now received new scanners. The software has been tested and is compatible with the current existing scanners. We are just waiting for some additional protective cases then will be starting a trial of the scanners. Check security of the system with Asset Management provider and see if additional security measures should be implemented immediately before new hardware. **Officer responsible:** Station Commander Research & Development **Date to be implemented by:** May 2021

Finding 10: Management Information – Stock checks	Risk Rating	Agreed Management Actions
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. 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.	**M**	**Action:** A stock level report was sent to finance when it was identified that a formal stock check wouldn't be achievable due to Covid-19. Arrange for internal audit/stock check to be carried out of stores and mezzanine area. **Officer responsible:** Asset Management and Equipment Manager **Date to be implemented by:** July 2021

Appendix 1: Definition of Conclusions

Key for the Overall Conclusion:

Below are the definitions for the overall conclusion on the system of internal control being maintained.

Definition		Rating Reason
Substantial	There is a sound system of internal control designed to achieve objectives and minimise risk.	The controls tested are being consistently applied and risks are being effectively managed. Actions are of an advisory nature in context of the systems, operating controls and management of risks. Some medium priority matters may also be present.
Reasonable	There is a good system of internal control in place which should ensure objectives are generally achieved, but some issues have been raised which may result in a degree of risk exposure beyond that which is considered acceptable.	Generally good systems of internal control are found to be in place but there are some areas where controls are not effectively applied and/or not sufficiently developed. Majority of actions are of medium priority but some high priority actions may be present.
Partial	The system of internal control designed to achieve objectives is inadequate. There are an unacceptable number of weaknesses which have been identified and the level of non-compliance and / or weaknesses in the system of internal control puts the system objectives at risk.	There is an inadequate level of internal control in place and/or controls are not being operated effectively and consistently. Actions may include high and medium priority matters to be addressed.
Limited	Fundamental weaknesses have been identified in the system of internal control resulting in the control environment being unacceptably weak and this exposes the system objectives to an unacceptable level of risk.	The internal control is generally weak/does not exist. Significant non-compliance with basic controls which leaves the system open to error and/or abuse. Actions will include high priority matters to be actions. Some medium priority matters may also be present.

Management actions have been agreed to address control weakness identified during the exit meeting and agreement of the draft Internal Audit report. All management actions will be entered onto the Pentana Performance Management System and progress in implementing these actions will be tracked and reported to the Strategic Management Board and the Overview & Audit Committee.

We categorise our management actions according to their level of priority:

Action Priority	Definition
High (H)	Action is considered essential to ensure that the organisation is not exposed to an unacceptable level of risk.
Medium (M)	Action is considered necessary to avoid exposing the organisation to significant risk.
Low (L)	Action is advised to enhance the system of control and avoid any minor risk exposure to the organisation.

Appendix 2: Officers Interviewed

The following staff contributed to the outcome of the audit:

Name:	Title:
Mark Hemming	Director of Finance and Assets
Marcus Hussey	Principal Accountant
Carl Hayward	Station Commander Research & Development
Tony Hart	Asset Management Technician
Chris Cook	Asset Management Technician
Laura Taylor	Principal Accountant
Jess Bunce	Trainee Accountant
Ronda Smith	Procurement Manager
Gordon Wylie	Property Manager
Rob Spearing	Facilities Manager

The Exit Meeting was attended by:

Name:	Title:
Maria Darrell	Asset Management and Equipment Manager
Carl Hayward	Station Commander Research & Development
Tony Hart	Asset Management Technician

The auditors are grateful for the cooperation and assistance provided from all the management and staff who were involved in the audit. We would like to take this opportunity to thank them for their participation.

Appendix 3: Distribution List

Draft Report:

Mark Hemming	Director of Finance and Assets
Carl Hayward	Station Commander Research & Development
Maria Darrell	Asset Management and Equipment Manager
Gordon Wylie	Property Manager

Final Report as above plus:

Jason Thelwell	Chief Fire Officer
Ernst and Young	External Audit

Audit Control:

Closing Meeting	7 January 2020
Draft Report	11 January 2021
Management Responses	15 January 2021
Final Report	23 February 2021
Audit File Ref	21-10

Disclaimer

Any matters arising as a result of the audit are only those, which have been identified during the course of the work undertaken and are not necessarily a comprehensive statement of all the weaknesses that exist or all the improvements that could be made.

It is emphasised that the responsibility for the maintenance of a sound system of management control rests with management and that the work performed by Internal Audit Services on the internal control system should not be relied upon to identify all system weaknesses that may exist. However, audit procedures are designed so that any material weaknesses in management control have a reasonable chance of discovery. Effective implementation of management actions is important for the maintenance of a reliable management control system.

Contact Persons

Maggie Gibb, Head of Business Assurance

Phone: 01296 387327

Email: Maggie.gibb@buckinghamshire.gov.uk

Selina Harlock, Audit Manager

Phone: 01296 383717

Email: selina.harlock@buckinghamshire.gov.uk

APPENDIX D

Business Assurance and Risk Management

BMKFA Resource Management Application (FSR) Audit Report - FINAL (Ref-21/20)

Auditors

Maggie Gibb, Head of Business Assurance (and Chief Internal Auditor)

Selina Harlock, Audit Manager

Martin Baird, Mazar Director

Joseph Lennon, Mazars Associate Consultant

CONTENTS

Management Summary

Introduction

This audit of the Resource Management application at Buckinghamshire and Milton Keynes Fire Authority (hereby the Authority) was undertaken as part of the 2020/21 Internal Audit plan as approved by the Overview and Audit Committee. The audit was undertaken during the third quarter of 2020/21.

The purpose of the Authority is to provide Fire & Rescue Services in the South East region of England. The areas covered by the Authority reach the outskirts of London to the South Midlands which can be split into five geographical districts: Aylesbury Vale, Chiltern, South Buckinghamshire, Wycombe and Milton Keynes.

The Authority have recently changed their Resource Management application to an application known as Fire Service Rota (hereby FSR) which went live in April 2020. FSR was implemented as part of numerous projects to move to flexible and affordable crewing systems. FSR itself was chosen as it aligned with the Authority's new method of resourcing on-call appliances, which will eventually interface directly into the Authority's mobilising system (Vision).

FSR is provided by the Vendor (known as FSR itself) on a contract that is a 'semi-managed service'. This means that several processes/controls are operated by the Vendor (such as change and incident management) with other controls operated by the Authority themselves (such as user access management). Such controls are operated by a small team within the Authority known as the Resource Management Team (hereby RMT). Vendor operated controls for change and incident management are managed through the Vendor's service desk Zendesk.

Audit Objective

Internal Audit's objectives for this audit are to provide an evaluation of, and an opinion on, the adequacy and effectiveness of the system of internal controls that are in place to manage and mitigate financial and non-financial risks of the system.

This will serve as a contribution towards the overall opinion on the system of internal control that the Chief Internal Auditor is required to provide annually. It also provides assurance to the Section 151 officer that financial affairs are being properly administered.

Scope of work

The audit activity focussed on the following key risk areas identified in the processes relating to the FSR:

- Logical Access Controls
- Change Controls
- IT Operations

The audit considered the controls in place at the time of the audit only. Where appropriate testing was undertaken using samples of activities that occurred since the start of the 2020-21 financial year.

Table 1: Overall Conclusion

Overall conclusion on the system of internal control being maintained	**Partial**

RISK AREAS	AREA CONCLUSION	No of High Priority Management Actions	No of Medium Priority Management Actions	No of Low Priority Management Actions
Logical Access Controls	**Reasonable**	**0**	**2**	**2**
Change Controls	**Reasonable**	**0**	**2**	**0**
IT Operations	**Partial**	**1**	**1**	**0**
Total:		**1**	**5**	**2**

Appendix 1 provides a definition of the grading for each of the conclusions given.

Logical Access Controls

Logical access controls for the FSR application are mostly operated by the Authority with the exception of password controls. The RMT are the team assigned to manage access to this application and are the only team that can create new users or amend access via the 'Owner' role, with access to this role verified to be only held by members of the RMT.

There is no formalised user access procedure in place at the Authority detailing the processes involved when a user joins, moves or leaves the organisation. Tickets are raised on the Authority's Service Desk (Vivantio) when a user joins, moves within, or leaves the business and are sent to the RMT inbox to be addressed.

These tickets are either closed soon after an operator has seen and addressed the ticket. The ticket captures information such as the joiner's name, start date, employee number and job title but does not consider to what level of access the users should have, as sometimes users need access to multiple teams or rotas with different role types.

Generic accounts are kept to a minimum and usernames for users are in the main attributable on the application, although some generic accounts exist which appear to not be in use. Furthermore, the Authority does not have access to the database or OS.

User access reviews are not undertaken performed on a periodic basis except for a review in July 2020, whereby lists of user accounts were sent to Supervisory managers (based on the rota or team they supervise) to ensure those users should have access to their rota/team/cluster and the role they have at said level.

Users are required to authenticate their access using a username and password before they are allowed access to the application. The password parameters are not currently under the Authority's control. FSR utilises 'Rumkin' password strength checker to ensure passwords are strong. This works by utilising the concept of entropy (measure of randomness).

Currently, password entropy is set to be 40 bits or higher which is considered a moderately strong password. Items such as using commonly used passwords, words or phrases, short length, or common combinations of letters will cause password entropy to decrease and not meet the criteria. Although 40 bits is considered moderate and appropriate for network and company resources, the Authority has no granular control over password parameters. Password controls are hard coded into the application and cannot be changed.

Change Controls

The vast majority of change controls are operated by the Vendor. Irrespective, an internal change control process exists at the Authority. Changes are to be raised through the Vivantio service desk by a change initiator and must include key information such as:

- Business case supporting the change;
- Cost estimates;
- Any potential risks;
- Estimation of resources required;
- Budget associated; and
- Time schedule.

The change is then assessed by the Change Manager/Change Advisory Board (CAB)/Emergency Change Advisory Board (ECAB) to ensure that the previously defined areas are considered in the request for change. Once the change has been assessed by the relevant stakeholders, the change is approved to be developed.

The change is communicated to the Vendor through their Zendesk service desk who will then develop the change based on the agreed timescale and conduct all testing. Discussions with the Vendor established that over 1000 automated tests are ran on FSR every time a change is made to the application.

The Vendor will also perform specific targeted tests as part of user acceptance testing (UAT) to ensure the new change is functioning/operating in the correct way. The Authority does not have access to a test environment and hence all testing including user acceptance testing is conducted by the Vendor. It was also noted that authorisation is provided to the Vendor to make the change to the live system once the Vendor confirms that the change is ready. Although authorisation is given by the Authority, the Authority has 'no part to play' in the process thus making the approval irrelevant.

IT Operations

In order to calculate the renumeration payable to employees, a batch-job process runs outbound of FSR for payroll extracts used by HR. This process is semi-automated in the sense that the system produces the report but is required to be initiated by the Payroll Manager. It was noted that assurance is gained over the integrity of output of the reports from the initial project work (i.e. the system implementation).

Underlying rules for applying working time and pay rules were all considered during the deployment project of FSR. Furthermore, there are various checks and reviews completed by the Payroll Manager and other members of the Payroll Team to ensure that the data extracted out of FSR is complete and accurate before applying the data to pay records.

Responsibility for backups of the application and its underlying database is controlled and operated by the Vendor. There are two types of backups ran, with one being a snapshot backup performed every 12 hours whereby the entire database is stored as a single file. This file is encrypted, stored to an Amazon S3 EU datacentre, and stored for 30 days. The second type of backup ran is a streaming backup. This is performed continuously, and data is stored in an Amazon S3 EU Datacentre in an encrypted format. In case of a failure, these streaming backups are at most a few minutes behind the live data.

Disaster recovery (DR) is considered within the vendor's Business Continuity Plan and states that a full-scale disaster recovery process has been developed and tested. Noted from previous tests, the entire DR process can be executed in as little as five hours. We were unable to obtain evidence that DR tests had been conducted on behalf of the Authority by the Vendor. This emphasises the need for the Authority to obtain formal assurance over the controls/processes operated by the vendor.

It was noted that service reviews are held monthly between FSR and the Authority. No formalised meeting minutes or documents are maintained as part of these reviews and the meetings held informally held to discuss customer service-based issues. Service reviews can provide a high level of assurance over the controls operated by the vendor and should be obtained by the Authority to reduce the risks associated with the controls operated by the Vendor. We noted that the Authority gain no formal assurance (such as a Service Organisation Controls (SOC) report or ISO27001 certification) from the Vendor.

Table 2: Detailed Audit Findings and Management Action Plan

Finding 1: Service Reviews	Risk Rating	Agreed Management Actions
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. 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).	**H**	**Action:** Assurance to be sought from the vendor regarding efficacy of risk controls, especially in relation to cyber security. **Officer responsible:** Station Commander RMT **Date to be implemented by:** June 2021
Finding 2: Joiners, Movers and Leavers Policy/Procedure	**Risk Rating**	**Agreed Management Actions**
The Authority does not have a formalised user access management process outlining the processes/controls when a user joins, moves or leaves the organisation and the relevant user access requirements. 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. Unauthorised access to company resources may lead to loss and compromise of data.	**M**	**Action:** A review of the processes will be undertaken, supported by the end-to-end process mapping within the Internal Audit Plan for 2021-22. **Officer responsible:** Station Commander RMT **Date to be implemented by:** December 2021

Finding 3: Generic Accounts	Risk Rating	Agreed Management Actions
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. There could be a loss of accountability of user performed actions. Unauthorised access to company resources may lead to loss and compromise of data.	**M**	**Action:** A review of user accounts to be undertaken and redundant generic accounts to be removed. **Officer responsible:** Station Commander RMT **Date to be implemented by:** June 2021
Finding 4: Change Management - Testing	**Risk Rating**	**Agreed Management Actions**
The vast majority of change controls are operated by the Vendor. Irrespective, an internal change control process exists at the Authority. Changes are to be raised through the Vivantio service desk by a change initiator and must include key information However, we noted that: • 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. 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.	**M**	**Action:** Change management process to be reviewed and fully documented (see also Finding 5). **Officer responsible:** Station Commander RMT **Date to be implemented by:** September 2021

Finding 5: Change Management – Internal Tracking and Assessment	Risk Rating	Agreed Management Actions
All changes are required to pass through the change management process with a request for change (RfC) document completed for each change. 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 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.	**M**	**Action:** Change management process to be reviewed and fully documented (see also Finding 6). **Officer responsible:** Station Commander RMT **Date to be implemented by:** September 2021
Finding 6: Backups – Disaster Recovery Testing	**Risk Rating**	**Agreed Management Actions**
Backups and the associated disaster recovery procedures are controlled and operated by the Vendor. 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. There is a risk of partial or complete loss of data. Unavailability of systems and lack of business continuity.	**M**	**Action:** A disaster recovery will be undertaken to test business continuity in this area. **Officer responsible:** Station Commander RMT **Date to be implemented by:** September 2021
Finding 7: User Access Reviews	**Risk Rating**	**Agreed Management Actions**
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. There is a risk of inappropriate access to the Authority's resources.	**L**	**Action:** User access to be reviewed every six months. **Officer responsible:** Station Commander RMT **Date to be implemented by:** September 2021

Finding 8: Password Configuration	Risk Rating	Agreed Management Actions
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. There is a risk of unauthorised access to company resources due to weak password configuration, which increases the likelihood of a brute force attack.	**L**	**Action:** Potential updating of the password configuration to be discussed with the supplier. **Officer responsible:** Station Commander RMT **Date to be implemented by:** March 2022

Appendix 1: Definition of Conclusions

Key for the Overall Conclusion:

Below are the definitions for the overall conclusion on the system of internal control being maintained.

Definition		Rating Reason
Substantial	There is a sound system of internal control designed to achieve objectives and minimise risk.	The controls tested are being consistently applied and risks are being effectively managed. Actions are of an advisory nature in context of the systems, operating controls and management of risks. Some medium priority matters may also be present.
Reasonable	There is a good system of internal control in place which should ensure objectives are generally achieved, but some issues have been raised which may result in a degree of risk exposure beyond that which is considered acceptable.	Generally good systems of internal control are found to be in place but there are some areas where controls are not effectively applied and/or not sufficiently developed. Majority of actions are of medium priority but some high priority actions may be present.
Partial	The system of internal control designed to achieve objectives is inadequate. There are an unacceptable number of weaknesses which have been identified and the level of non-compliance and / or weaknesses in the system of internal control puts the system objectives at risk.	There is an inadequate level of internal control in place and/or controls are not being operated effectively and consistently. Actions may include high and medium priority matters to be addressed.
Limited	Fundamental weaknesses have been identified in the system of internal control resulting in the control environment being unacceptably weak and this exposes the system objectives to an unacceptable level of risk.	The internal control is generally weak/does not exist. Significant non-compliance with basic controls which leaves the system open to error and/or abuse. Actions will include high priority matters to be actions. Some medium priority matters may also be present.

Management actions have been agreed to address control weakness identified during the exit meeting and agreement of the draft Internal Audit report. All management actions will be entered onto the Pentana Performance Management System and progress in implementing these actions will be tracked and reported to the Strategic Management Board and the Overview & Audit Committee.

We categorise our management actions according to their level of priority:

Action Priority	Definition
High (H)	Action is considered essential to ensure that the organisation is not exposed to an unacceptable level of risk.
Medium (M)	Action is considered necessary to avoid exposing the organisation to significant risk.
Low (L)	Action is advised to enhance the system of control and avoid any minor risk exposure to the organisation.

Appendix 2: Officers Interviewed

The following staff contributed to the outcome of the audit:

Name:	Title:
Andrew Holtzhausen	Station Commander RMT
Adam Burch	Station Commander Projects
Sharon Elmes	Payroll and Benefits Manager
Colin Partridge	RMT Watch Commander
Rebeca Gutierrez	Customer Success Leader (FSR)

The Exit Meeting was attended by:

Name:	Title:
Andrew Holtzhausen	Station Commander RMT

The auditors are grateful for the cooperation and assistance provided from all the management and staff who were involved in the audit. We would like to take this opportunity to thank them for their participation.

Appendix 3: Distribution List

Draft Report:

Andrew Holtzhausen	Station Commander RMT
Adam Burch	Station Commander Projects
Sharon Elmes	Payroll and Benefits Manager
Colin Partridge	RMT Watch Commander
Rebeca Gutierrez	Customer Success Leader (FSR)

Final Report as above plus:

Mark Hemming	Director of Finance and Assets
Jason Thelwell	Chief Fire Officer
Ernst and Young	External Audit

Audit Control:

Closing Meeting	22 February 2021
Draft Report	2 February 2021
Management Responses	23 February 2021
Final Report	24 February 2021
Audit File Ref	21-20

Disclaimer

Any matters arising as a result of the audit are only those, which have been identified during the course of the work undertaken and are not necessarily a comprehensive statement of all the weaknesses that exist or all the improvements that could be made.

It is emphasised that the responsibility for the maintenance of a sound system of management control rests with management and that the work performed by Internal Audit Services on the internal control system should not be relied upon to identify all system weaknesses that may exist. However, audit procedures are designed so that any material weaknesses in management control have a reasonable chance of discovery. Effective implementation of management actions is important for the maintenance of a reliable management control system.

Contact Persons

Maggie Gibb, Head of Business Assurance

Phone: 01296 387327

Email: maggie.gibb@buckinghamshire.gov.uk

Selina Harlock, Audit Manager

Phone: 01296 383717

Email: selina.harlock@buckinghamshire.gov.uk