Buckinghamshire & Milton Keynes Fire Authority

Meeting and date: Overview and Audit Committee, 15 March 2023

Report title: Internal Audit Report – Final Audit Reports

Lead Member: Councillor David Carroll

Report sponsor: Mark Hemming – Director of Finance and Assets

Author and contact: Maggie Gibb – Chief Auditor, Maggie.Gibb@buckinghamshire.gov.uk, 01296 387327

Action: Noting.

Recommendations: That Members note the final audit reports for FY 2022/23

Executive summary: The purpose of this paper is to update Members on the progress of the annual Internal Audit Plan since the last meeting.

Work has progressed according to the approved 2022/23 plan, and regular discussions have been held with the Director of Finance and Assets to monitor progress.

The following 2022/23 internal audits have been finalised:

- Core Financial Controls (Substantial Opinion)
- Business Continuity and Risk Management (Reasonable Opinion)
- Pension Fund Administration (Substantial Opinion)
- HR/Payroll Process Mapping (Assurance Opinion is not applicable)

From discussion with the Director of Finance and Assets, it has been agreed that the Inspection and Operational Improvement Plan Assurance review will be undertaken as part of the FY 2023/24 Internal Audit Plan.

Financial implications: The audit work is contained within the 2022/23 budget.

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

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

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

Duty to collaborate: Not applicable.

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

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

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

Consultation and communication: Not applicable.

Background papers:

Appendix	Title	Protective Marking
A	Core Financial Controls Audit Report	Not applicable
B	Business Continuity and Risk Management Audit Report	Not applicable
C	Pension Fund Administration Audit Report	Not applicable
D	HR/Payroll Process Mapping Assurance	Not applicable

Business Assurance and Risk Management

Core Financial Controls Audit Report - FINAL (Ref-23/06)

Auditors

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

Selina Harlock, Audit Manager

Alex Prestridge, Senior Auditor

Management Summary

Introduction

The audit of Core Financial Controls was undertaken as part of the 2022/2023 Internal Audit plan which was approved by the Overview and Audit Committee.

The Core Financial Controls Audit reviewed the Fire Authority's key financial processes, including Creditors, Debtors, 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 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 internal control system 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 covering the period between December 2021 and November 2022. The implementation of management actions raised from previous audits was also reviewed as part of the audit.

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	**Reasonable**	0	0	1
Creditors	**Reasonable**	0	0	1
Debtors	**Substantial**	0	0	0
Payroll	**Reasonable**	0	0	1
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	0	3

Appendix 1 defines the grading for each of the conclusions given.

Financial Control Framework

The Financial Regulations were updated in September 2019, reflecting current procurement limits, and were up to date. 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. They are reviewed and updated to reflect changes to the Finance system. However, we noted that these have not been reviewed for five years, whereas best practice suggests that they are reviewed regularly as well as when known changes are implemented (**Finding 2**).

We also reviewed the contract Standing Orders (CSOs). These were updated in December 2022 and include hyperlinks to procurement limits and relevant legislation, ensuring these remain up to date.

Process notes were reviewed for all key financial processes, 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 an 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 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.

Requisitioner roles can create requisitions and Budget Holders can authorise requisitions via workflows. Requisitions are then turned into a purchase order (POs) and sent to the supplier via email. System parameters on Integra force 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 transactions higher in value than their assigned limit.

Examination of a sample of 25 supplier invoices paid between December 2021 and November 2022 found that:
- In all 25 cases, the invoice was authorised for payment in line with delegated approval limits. All demonstrated an adequate segregation of duties.
- In all 25 cases, the purchase order was raised before the date of the invoice.
- In all 25 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.

- 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.

A sample of six credit notes received between December 2021 and November 2022 was selected from the Purchase Ledger Transactions Report.

Examination established that:
- For all six credit notes reviewed, the credits were allocated to the correct supplier.
- In all six 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 Assistant confirmed that changes are made as a result of an email request. If the change involves a change of bank details, the Finance Assistant 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 Principal Accountant for final independent approval, with emails saved on Integra's supplier records.

Examination of a sample of five new vendors and four changes to existing records for the period between December 2021 November 2022 found no exceptions, with all new vendors and changes appropriately approved with an adequate separation of duties, and supporting documentation retained.

Examination of a sample of five weekly BACS runs for the period between December 2021 and November 2022 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 December 2021 to November 2022 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 showed that 62 staff hold Purchasing Cards, with 61 of these having been activated. 60 cardholders used their purchasing cards between 1 December 2021 and 30 November 2022. Of these, one did not appear on the list of purchasing card holders. Discussion and review of a list of recent leavers confirmed that this was due to them leaving the Fire Authority's employment. Review of transactions for the period found that no purchases were made using the card after their leave date.

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 December 2021 and November 2022 found:

- In all 20 cases, a valid proof of purchase was retained.
- In all 20 cases, the amount on the receipt matched that on the bank statement and that recorded on Integra.
- In all 20 cases, use of the card was in line with the Financial Instructions and Purchasing Card User Guide.
- In 12 cases, purchases were made within the cardholder's designated spending limit. In six cases, total spend for the month of the transaction was not within the cardholder's monthly spending imit. In one of these cases, a single purchase of £2,248 exceeded the cardholder's spending limit of £1,000. In all six cases, a temporary increase to the cardholder's spend limit was approved by the line manager then actioned by Finance. For the remaining two transactions (both made by the same cardholder), the cardholder was not included on the list of purchasing card holders provided as they had left the Fire Authority's employment. However, we confirmed that no purchases were made using the card following the employee's leave date. Analysis of all Purchasing Card transactions by cardholder, found 16 instances where monthly spend was higher than the designated spend limit in the period between 1 December 2021 and 30 November 2022. Discussion with the Principal Accountant agreed that Purchasing Card limits are in need of review and that the purchasing card limits by organisational role set out in the Purchasing Card User Guide should also be reviewed to take into account positions and limits not previously listed (**Finding 1**).

Debtors

Financial Instructions include guidance for the Accounts Receivable functions. Documented procedures for Debtors processes and how these are actioned on Integra were obtained. They were found to be up to date and available to staff in the shared area. We confirmed that access to set up customers is restricted to members of the Finance team.

A report of invoices raised between December 2021 and November 2022 was obtained from the Principal Accountant. There were 290 invoices raised over the period.

Examination of a sample of 25 debtor invoices raised on Integra between December 2021 and November 2022 found:

- In all 25 cases, the invoice had been booked to an appropriate budget and General Ledger code.
- Where purchase orders would be expected, these were viewed, and details agreed to the corresponding invoice.
- In all 25 cases, invoices were confirmed as having been input by Finance staff with adequate separation of duties.
- In 16 cases, the invoice was paid within the Fire Authority's payment term of 14 days. In nine cases the invoice had not been paid within 14 days, although all nine had evidence of chasing.

A report of Credit Notes was run from Integra listing six credit notes raised between December 2021 and November 2022. Testing found that:

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

- In all six cases, the amount and customer match those on the original 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 2022, there was a total of £253,379 outstanding debt owed to the Authority, of which £246,312.43 was over 60 days old. Of this, £239,263 related to SCAS rental, Buckinghamshire Council, National Trust and Babcock International. We noted the Authority's debt profile had increased significantly over the period from December 2021, when there were total debts outstanding of £59,041.05. We confirmed that all debt was being chased in line with the Fire Authority's debt recovery process. It was confirmed that there were no write-offs for 2021/22. The outstanding invoice of £239,263 relating to SCAS rental has since been settled on 06 February 2023.

Payroll

Payroll information is processed through the iTrent system. The Fire Service Rota (FSR) planning and scheduling system is used to record all Watch-based inputs.

Examination of a sample of ten new starters for the December 2021 to November 2022 period confirmed that:

- In all cases, the payroll details were correctly entered on iTrent with an adequate separation of duties. The appropriate authorisations were obtained.
- In nine cases, a new starter checklist was completed. In one case, a new starter checklist was not completed. Further investigation found that the employee's start and end date were the same, with a leaver notification received before the start date and before Payroll would have started processing the new starter. This was therefore not deemed to be an issue.

Examination of a sample of ten permanent changes made to payroll between December 2021 and November 2022 found:

- In all ten cases, authorisation for the change was held on file.
- In all ten cases, the change matched the employee's information on iTrent.
- In six cases, there was evidence that the Change Control Form and change in iTrent were checked by a second officer. In four cases, there was no evidence of a check by a second officer (**Finding 3**).

An up to date Expenses Policy was in place, providing guidance to officers around claiming expenses and mileage. Examination of a sample of 20 expenses and mileage payments made to staff between December 2021 and November 2022 found no exceptions.

Examination of a sample of ten overtime payments made to staff between December 2021 and November 2022 found:

- In all ten cases, a claim form was completed either via iTrent's ESS module or via FSR and approved by the employee's line manager.
- In all ten cases, the overtime paid on the employee's payslip matched the claim form and amount accounted for on Integra.
- In all ten cases, the overtime was paid in the month the claim was authorised.

Examination of a sample of ten employees who left the Fire Authority's employment between December 2021 and November 2022 found:

- In all ten cases, leaver notification was received prior to the employees leave date.
- We confirmed by viewing iTrent via the Payroll Managers screen that in all ten cases recurring payments were deleted.
- In all ten cases, a leaver form was completed.
- In six cases, a payroll leaver's checklist was completed and checked by a second officer. However, in four cases there was no evidence on the checklist that a second check was carried out (**Finding 3**).

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.

A total of 149 journals were raised between December 2021 and November 2022. Examination of a sample of 20 journals found that:

- In all 20 cases, journals were entered and authorised with an adequate segregation of duties.
- All journals were found to agree to backing documentation.

Grant Income

We reviewed schedules of expected grant income for 2022/23 provided to the Fire Authority by the authorities and Government departments awarding them. We noted that a schedule of payments was provided by Buckinghamshire Council for 2022/23, showing a total Council Tax precept payment of £16,166,750.20.

Expected grants for 2022/23 were the Services Grant, BRRS (Business Rates Relief Reimbursement), RSG (Revenue Support Grant), Fire Pensions Grant, Protection Grant, New Dimensions Grant, Firelink Grant and the agreed 2022/23 Council Tax Precept from both Buckinghamshire Council and Milton Keynes Council.

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

- In all five cases, the income expected was received on the expected date.
- In all five cases, the amount received as shown on the bank statement and Integra agrees with the schedule.
- 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.

Capital

The Capital Programme for 2022-23 to 2026/27 was approved as part of the MTFP at the Executive Committee meeting on 9 February 2022 and Fire Authority on 16 February 2022. The agreed capital budget for 2022/23 was £2,426,000, with an approved revised budget of £3,939,500 as at October 2022.

Assets are valued annually by Bruton Knowles. A copy of the valuation report produced in March 2022 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 2021/22 totalled £276,380, as per the Asset Register. This included £7,400 of Red Fleet disposals, £100,756 of White Fleet disposals and £168,224 of plant and equipment disposals. There were no recorded land or building disposals for 2021/22. We found that all disposals were appropriately approved.

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 Assistant 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 from bank statements for April, August, June, October, and September 2022. In all five cases, we found that the creditor and payment amount matched that listed on Integra.

We also selected a sample of five income transactions recorded on 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

A review of the VAT returns report generated from Integra covering the period between April and October 2022 confirmed that the reconciliation for these was reviewed and agreed to each month's sales ledger and Purchase Ledger VAT amounts. These were then agreed to the control account.

A walkthrough of the process was viewed during the preparation and authorisation of the returns for September and October 2022. For both months, the Finance Assistant created the report, which was checked and authorised by the Principal Accountant and submitted to HMRC using unique log-in details.

Treasury Management

The Treasury Management Strategy for 2022-23 was approved at the Fire Authority meeting on 16 February 2022. The Strategy refers to CIPFA best practice and guidance on prudential investments and DLUHC 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. Counterparties are agreed as part of the Treasury Management Strategy and are based on the advice received from the contracted treasury advisors.

Link Treasury Services provide regular weekly updates of credit ratings for counterparties to BMKFA and a monthly Investment Analysis Review. We confirmed that there is a signed contract with Link Treasury Services for Treasury Management Advisory services. In line with the terms and conditions as well as the Contract Standing Orders, the contract with Link Treasury Services which was due to expire in March 2022, was extended to 31 March 2024.

Management reports are produced quarterly by the Principal Accountant and presented to the Overview and Audit Committee. For 2022-23 Quarter 2, the report showed that the accrued interest earned for the first half of 2022-23 was £83k, which was £68k higher than the budgeted amount of £15k for the same period.

A report was obtained of deals executed between 1 April 2022 and 30 November 2022 from Treasury Live. This shows all investment deals made, matured investments, and movements in money market funds (MMF). There were 23 Fixed deals, seven MMF deals and nine call deals made over this period. No exceptions were noted, with no counterparty limits having been breached.

Table 2: Detailed Audit Findings and Management Action Plan

Finding 1: Creditors – Purchasing card spending limits	Risk Rating	Agreed Management Actions
Purchasing card holders are assigned a monthly spending limit in line with the requirements of their role. These should be periodically reviewed to ensure that they continue to be in line with the requirements of officers' roles. Examination of a sample of 20 purchasing card transactions found: • In six cases, total spend for the month of the transactions was not within the cardholder's monthly spending limit. In one of these cases, a single purchase of £2,248 exceeded the cardholder's spending limit of £1,000. Whilst a temporary increase to the cardholders' spend limit was approved by the budget holder and actioned by Finance in all six cases, and all spend was within the temporary increase to the limit, analysis of all Purchasing Card transactions found 16 instances (spread across ten cardholders) where monthly spend was higher than the designated spend limit in the period between 1 December 2021 and 30 November 2022, indicating that the officers were exceeding their limits with relative frequency. Discussion with the Principal Accountant agreed that Purchasing Card limits are in need of review and that the purchasing card limits by organisational role set out in the Purchasing Card User Guide should also be reviewed to take into account positions and limits not previously listed. If purchasing card spend limits do not reflect actual purchasing card spend, there is a risk that temporary increases to spend limits become increasingly frequent, leading to inconsistent purchasing card usage across the Fire Authority.	L	**Action:** A Review of the Purchasing Card User Guide to ensure the guide is still fit for purposes and purchasing card limits are sufficient and appropriate for all purchasing card holders. **Officer responsible:** Principal Accountant **Date to be implemented by:** 30 June 2023
Finding 2: Financial Control Framework – Financial Instructions	Risk Rating	Agreed Management Actions
Financial Instructions should cover all financial processes, be up to date, approved and made available to staff. We noted that the Financial Instructions document was last updated and approved in January 2018 and has therefore not been reviewed for five years, whereas best practice suggests that financial policies and procedures are reviewed regularly as well as when known changes are implemented.	L	**Action:** A review and update of the Financial Instructions to take place to incorporate actions from the Procurement Audit. **Officer responsible:**

	Risk Rating	
If Financial Instructions are not kept under regular review there is a risk that they are not up to date and do not reflect the current operations and strategic objectives of the Fire Authority, as well as any changes to legislation.		Director of Finance and Assets **Date to be implemented by:** 31 March 2023
Finding 3: Payroll – Second officer check	**Risk Rating**	**Agreed Management Actions**
Information relating to permanent changes and leavers should be input by an HR or Payroll Officer and checked by a second Payroll Officer. Examination of a sample of ten permanent changes made to payroll between December 2021 and November 2022 found that in four cases, there was no evidence that inputs relating to the change were checked by a second officer. Examination of a sample of ten employees who left the Fire Authority's employment between December 2021 and November 2022 found that in four cases there was no evidence on the checklist that a second check was carried out. If inputs into Integra are not checked by a second officer, there is a risk that permanent changes and leavers are processed incorrectly and the pay information is not accurate, leading to an overpayment or underpayment.	**L**	**Action:** As the team is now at full establishment and trained, these checks are taking place. **Officers responsible:** Payroll Manager **Date to be implemented by:** Immediately

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	A sound system of governance, risk management and control exist, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited.	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 generally sound system of governance, risk management and control in place. Some issues, non-compliance or scope for improvement were identified which may put at risk the achievement of objectives in the area audited.	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.
Limited	Significant gaps, weaknesses or non-compliance were identified. Improvement is required to the system of governance, risk management and control to effectively manage risks to the achievement of objectives in the area audited.	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.
No Assurance	Immediate action is required to address fundamental gaps, weaknesses or non-compliance identified. The system of governance, risk management and control is inadequate to effectively manage risks to the achievement of objectives in the area audited.	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 actioned. 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 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)
Laura Taylor	Principal Accountant (Management Accounting)
Jackie Vere-White	Payroll Manager
Raheel Iqbal	Finance Assistant

The Exit Meeting was attended by:

Name:	Title:
Asif Hussain	Deputy Director of Finance and Assets
Laura Taylor	Principal Accountant (Management Accounting)
Marcus Hussey	Principal Accountant (Technical Accounting)
Jackie Vere-White	Payroll 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
Laura Taylor	Principal Accountant (Management Accounting)
Marcus Hussey	Principal Accountant (Technical Accounting)
Jackie Vere-White	Payroll Manager

Final Report as above plus:

Jason Thelwell	Chief Fire Officer
Ernst and Young	External Audit

Audit Control:

Closing Meeting	3 February 2022
Draft Report	8 February 2022
Management Responses	10 February 2022
Final Report	10 February 2022
Audit File Ref	23-06

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

Business Assurance and Risk Management

Risk Management and Business Continuity Planning - FINAL

Auditors

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

Selina Harlock, Audit Manager

Juan Fosco, Audit Manager

Axolile Kopman, Assistant Manager

Management Summary

Introduction

The Business Continuity and Risk Management audit was undertaken as part of the 2022/23 Internal Audit plan. This area was included in the plan at the Audit Committee's request and due to the significance of risks related to the area in Buckinghamshire & Milton Keynes Fire Authority (BMKFA) Risk Register. Under the Civil Contingencies Act 2004, the Authority has a statutory duty to maintain business continuity plans to ensure they can maintain services in the event of an emergency.

Due to the reliance placed on ICT for the operation of services within the Authority, ICT service resilience and disaster recovery provisions are critical components of business continuity. Disaster Recovery (DR) planning enables the recovery of ICT systems in the event of disruption impacting the data centre or server room hosting the Authority's IT systems. Given that information and communication technology plays an increasingly important role in delivering Authority services, the ability to recover these systems promptly is essential.

Audit Objective

Internal Audit's objectives for this audit were to provide an evaluation of, and an opinion on, the adequacy and effectiveness of current controls over Risk Management and Business Continuity Planning and guide how to improve the current controls going forward.

This will serve as a contribution toward 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 agreed scope of this audit was:

- Risk Management Framework;
- Risk Identification and Evaluation;
- Risk Record and Management;
- Risk Monitoring;
- Policies, Procedures & Business Continuity Plans;
- Roles & Responsibilities;
- Business Continuity Testing;
- Lessons Learned;
- Monitoring & Reporting;
- Anticipated Industrial Action Plans, and
- ICT Disaster Recovery.

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

Table 1: Overall Conclusion

Overall conclusion on the system of internal control being maintained	Reasonable

RISK AREAS	AREA CONCLUSION	No. of High Priority Management Actions	No. of Medium Priority Management Actions	No. of Low Priority Management Actions
Risk Management				
Risk Management Framework	**Substantial**	0	0	0
Risk Identification and Evaluation	**Substantial**	0	0	0
Risk Record and Management	**Substantial**	0	0	0
Risk Monitoring	**Substantial**	0	0	0
Business Continuity Planning				
Policies, Procedures & Business Continuity Plans	**Reasonable**	0	1	0
Roles & Responsibilities	**Reasonable**	0	1	0
Business Continuity Testing	**Limited**	1	0	0
Lessons Learned	**Reasonable**	0	1	0
Monitoring & Reporting	**Reasonable**	0	1	0
Anticipated Industrial Action Plans	**Substantial**	0	0	0
ICT Disaster Recovery	**Limited**	1	0	1
Total		**2**	**4**	**1**

Appendix 1 defines the grading for each of the conclusions given.

Risk Management

Risk Management Framework

The Authority has a Corporate Risk Management Policy approved by the Fire Authority Executive Committee on 24 March 2021. Among others, the Policy sets out the following:

- Risk Management Definitions;
- Risk Appetite;
- Governance Structures;
- Roles and Responsibilities;
- Risk Management Processes and Methods;
- Consultation /Publication / Communication, and
- Impact Assessments.

The overall responsibility for risk management sits with the Authority's Strategic Management Board (SMB), which is responsible for reviewing, moderating and owning the risks designated as 'corporate'. The Chief Executive/Chief Fire Officer is responsible for day-to-day risk management.

The SMB has delegated responsibility to the Performance Monitoring Board (PMB) for reviewing and evaluating risks and acts as the escalation point for Directorate-level risks.

The Business Transformation Board (BTB) is also responsible for reviewing and evaluating risks and acts as the escalating point for project-related risks. Reviewing the Corporate Risk Management Policy and the Authority's Risk Registers, we confirmed that there is an appropriate delegation of risk management.

We confirmed that risk management is a regular agenda item at the relevant governance structures, such as the Strategic Management Board (SMB) and the Overview and Audit Committee (OAC). Reviewing the corporate risk management report prepared by the Corporate Planning Manager for the OAC meeting held in November 2022, we confirmed that risk management is covered and deliberated at the Authority's appropriate governance structures.

The Authority has a Public Safety Plan and the Corporate Plan for 2020-2025 that also informs the Authority's risk framework. For example, the Corporate Plan sets out strategic objective number four: *"To offer best value for money to our residents and businesses & ensure that the Service is compliant with regulatory requirements and recognised 'good practice' standards and can readily evidence this at all times"*. We confirmed that a risk was identified in the Corporate Risk Register concerning this strategic objective under Information Management/Security failure - to comply with statutory or regulatory requirements.

Risk Identification and Evaluation

The Corporate Risk Management Policy defines the risk appetite as the amount of risk the Authority is willing to tolerate relative to the size, nature, and degree of uncertainty associated with identified threats and opportunities. The Policy states that risks attracting a combined score of 20 or more on the Risk Scoring Matrix will be considered intolerable by the Authority and prioritised for treatment to eliminate or reduce the risk to acceptable levels. The Policy also indicates

that the ownership of the Risk Appetite at the Authority sits with the Fire Authority Executive Committee, and the risk appetite statement applies to the Authority at large. Reviewing the risk registers in place, we confirmed that for those risks that remained high after mitigating controls were suggested, further action plans were also suggested, and the actions are tracked as 'ongoing'.

Regarding training, we obtained a PowerPoint presentation on Corporate Risk Management utilised to provide training. The Corporate Planning Manager and the ICT Service Desk Manager conducted a specific training session in July 2021 for the new Members of the Fire Authority. Management confirmed that training is provided as and when there is a new starter joining the Authority. The training covers, amongst others:

- Risk management process;
- Risk scoring matrix, and
- Risk governance.

Upon our review of the Corporate Management Risk policy and risk registers, we noted that all grades of staff could identify risks. We also noted that the risks were escalated to the PMB should they require further action, and a responsible individual for managing the identified risk is assigned to the risk register.

Operational risk management is defined and coordinated. We reviewed the Directorate/corporate risk registers and confirmed that operational managers are responsible for managing operational risks by being assigned as risk owners.

Risk Recording and Management

Reviewing the Authority's risk registers, we confirmed that the risks were consistently scored using the quantitative approach method. The risks identified were assessed in terms of likelihood and severity (impact) for both inherent risk (gross risk) and residual risk (net risk). These were converted into numerical terms.

We reviewed the OAC reports and agendas for the 16 March, 20 July, and 09 November 2022 meetings. Upon review of the corporate risk register presented, we confirmed that action plans were suggested for the risks identified that required further action and were tracked on an ongoing basis. We confirmed this in the corporate risk management report the Corporate Planning Manager presented.

We reviewed the minutes of the Performance Monitoring Board (PMB) meeting held on 03 February, 09 June, and 29 September 2022. We noted that the risks escalated from the directorate management meetings were discussed. For example, on the 03 February 2022 meeting, a risk was escalated around information on Site Specific Risk Information (SSRI) and a further delay to the delivery of the related project.

We reviewed the extract of the meeting minutes of the Business Transformation Board (BTB) meeting held on 11 August, 08 September, and 06 October 2022. Upon review, we noted that the project risks escalated from the portfolio management office were discussed.

Reviewing the risk registers, we noted a clear distinction between types of risks. The risk registers were divided into prevention, response & resilience risk register, corporate risk register and directorate or departmental risk registers. We noted that the efforts SMB are focused on the Strategic risks, demonstrating appropriate prioritisation of senior management's time.

Corporate Planning provides appropriate templates and systems for analysing, evaluating, recording, and reporting risks identified at directorate and corporate levels. The Project Management Office (PMO) will do the same for project risks. We reviewed the directorate/departmental risk register, corporate risk register, and technology, transformation and PMO risk register, which highlighted that a systematic approach to risk management was continuously applied concerning risk identification, recording, assessment and analysis.

Risk Monitoring

Formal review and reporting of corporate risks are undertaken at every PMB and SMB meeting and the Authority's OAC. We reviewed the minutes of the PMB meetings held on 03 February, 09 June, and 29 September 2022. We confirmed that risk registers are reviewed and deliberated on this platform. We also reviewed the Board papers presented to the PMB corresponding to these meetings. The Board papers provided an update on the current status of identified corporate risks.

We also reviewed the extract of the meeting minutes for the Strategic Management Board (SMB) held on 23 August, 20 September, and 18 October 2022. The meeting minutes for 15 November 2022 were not yet available at the time of the audit; however, we reviewed the Board paper presented to the SMB, and we noted that risk registers are reviewed and deliberated in this platform. We also reviewed the Board papers presented to the SMB corresponding to these meetings and confirmed they provided an update on the current status of identified corporate risks.

Furthermore, we reviewed the minutes of the OAC meetings held on 16 March and 20 July 2022. Upon review, we noted that risk registers are reviewed and deliberated in this platform. We also reviewed the Board papers presented to the OAC corresponding to these meetings and confirmed they provided an update on the current status of identified corporate risks.

Business Continuity

Policies, Procedures & Business Continuity Plans

We reviewed the Business Continuity Policy and guidance (August 2022 version), which includes areas relevant to business continuity, including components such as the following:

- Production of the business continuity plans;
- Testing of the plans;
- Business continuity events, and
- Impact assessments.

As of December 2022, the Authority has 16 departments and 19 fire stations, each with a business continuity plan. We obtained copies of the plans for each department and fire station. We confirmed the existence, although we observed plans not being reviewed recently (more details are included in Table 2 below). Through the review of the business continuity policy, we also noted that the Authority pursues to align with the standards of Business Continuity Management as defined by ISO 22301 and the Business Continuity Institute Good Practice Guidelines.

Roles & Responsibilities

The Chief Fire Officer has ultimate responsibility for Business Continuity. This includes developing and implementing plans to anticipate, address and mitigate the effects of various business interruptions. The Resilience and Business Continuity Manager is tasked with the day-to-day roles and responsibilities regarding business continuity across the Authority. The job description for this role clearly states what is expected of the individual who occupies the role.

We obtained a copy of the Certificate of the Business Continuity Institute (CBCI) for the Resilience & Business Continuity Manager issued on 21/02/2020. The certification is valid for three years from the test's date and is subject to an annual maintenance fee.

Anticipated Industrial Action at the Authority

We obtained the industrial action plan (documented procedure), dated August 2022, and noted that it includes an appendix for 'industrial action planning'. This outlines what the Authority would do should the industrial action materialise. Also, industrial action planning is broken into a number of days as to what should happen on a particular day of a strike.

ICT Disaster Recovery

The Authority has an Information Communications (ICT) departmental business continuity plan issued in August 2022. The next review date is July 2023.

The Head of Technology, Transformation & PMO, the ICT Manager, and the ICT Service Desk Manager are responsible for ICT business continuity at the Authority. The Chief Fire Officer has ultimate responsibility for all aspects of Business Continuity.

The ICT Service Desk Manager is a nominated officer responsible for activating the ICT BCP during working hours. Out of hours or if none of the nominated persons is available, then the Duty Group Commander, in conjunction with the on-call ICT, will be contacted to decide if activation of the plan is appropriate.

We noted that as part of the ICT Disaster Recovery plan testing (last performed in 2019), lessons learned were identified due to the testing.

We were provided with the server screenshots and confirmed that ongoing backups are performed daily on data held within.

Table 2: Detailed Audit Findings and Management Action Plan

Finding 1: Business Continuity Plans - Testing	Risk Rating	Agreed Management Actions
We could not obtain evidence to support that the BCPs were tested annually as the business continuity guidance requires. Management indicated that this was not done due to capacity constraints in the business continuity section. Without developing and implementing a formal testing program, there is the risk that appropriate levels of testing are not undertaken to establish the ability of the BCP to support an effective and efficient response to business disruption. The lack of business continuity tests increases the risk that existing plans are not fit for purpose. The Authority would fail in its statutory duty to maintain services in an emergency or major incident. We recommend that, once all BCPs have been developed and approved, management introduce a risk-based testing program for BCPs. This should include a range of tests, including live testing and simulations of different scenarios. Testing must be targeted at areas most susceptible to an incident and/or would suffer the most adverse consequences. Plans should be confirmed as appropriate following the completion of tests.	H	**Action:** An exploratory testing programme, targeting those functions considered most at risk, will be developed and piloted during 23/24. Also, the options and associated costs and resources required to develop, implement, and sustain a fully recordable business continuity testing and exercising programme will be investigated during 23/24. **Officer responsible:** Station Commander Resilience & Business Continuity **Date to be implemented by:** 31 March 2024 for completion of pilot and review of future development options.
Finding 2: ICT Disaster Recovery Plan - Testing	Risk Rating	Agreed Management Actions
We confirmed that the ICT disaster recovery (DR) Plan was last tested in 2019. BMKFA should consider testing the ICT DR Plan annually to help the Authority identify and fix inconsistencies and flaws before they become full-blown problems. The authority should consider filling vacancies in the ICT in a timely manner to ensure that the unit is at full establishment to deliver on its tasks including Disaster Recovery Testing. BMKFA is faced with the risk of not being certain if the DR Plan is still functional, and also, there is a risk of missed opportunities.	H	**Action:** Vacant posts to be filled and ensure that ICT is at establishment. **Officer responsible:** ICT Manager **Date to be implemented by:** 31st March 2023 Latest Update: Two apprentices have been employed to assist with first line support, but it could take them up to 2 years to gain the correct skills and level of knowledge. **Action:** Test the ICT disaster recovery plan **Officer responsible:** ICT Manager **Date to be implemented by:** 31 March 2024

Finding 3: Business Continuity - Employee Awareness and Training	Risk Rating	Agreed Management Actions
We confirmed that the business continuity manager holds a Certificate of the Business Continuity Institute (CBCI). However, there has been limited awareness training provided for relevant staff (typically responsible managers) in relation to Business Continuity. Formal business continuity training is not developed and rolled out to responsible managers. This could be in the form of an e-Learning module. There is no active promotion by senior management to emphasise the importance of business continuity. This could be in the form of email campaigns or staff newsletters. If a positive business continuity culture is not embedded within the Authority, there is the risk that staff members will not have the required level of knowledge and will not fully understand their responsibilities effectively should BCPs be invoked.	M	**Action:** An e-Learning package will be developed in the short term. However, a full restructure of Business Continuity Management processes is required to fully meet the recommendations which will include the development and implementation of a business continuity awareness & training programme. **Officer responsible:** Station Commander Resilience & Business Continuity **Date to be implemented by:** 31 October 2023 (for the e-learning package) 31 March 2024 (for future development options / proposals).

Finding 4: Business Continuity Plans Review	Risk Rating	Agreed Management Actions
As of December 2022, the Authority had a total of sixteen directorates and nineteen fire stations; each had a BCP. Whilst the existence was confirmed, no evidence could be obtained that the BCPs were reviewed by the planned date. Management indicated an issue with the capacity of the business continuity section. Out of nineteen fire station BCPs, we noted that sixteen were not reviewed as planned:	M	**Action:** A full restructure of Business Continuity Management structures and processes is required to fully meet the recommendations which will include the development and implementation of fully auditable Business Continuity Plans that align to current standards and good practice. In the meantime, Business Continuity Plan review completions will be monitored on an ongoing basis and added to the suite of performance measures reported to the Authority's Executive Committee. **Officer responsible:** Station Commander Resilience & Business Continuity **Date to be implemented by:** Inclusion of BCP review completions in performance measures by 30 April 2023.

#	Fire Station	Issue Date	Planned Review Date
1	Amersham	14-Apr-21	12-Apr-22
2	Aylesbury	27-Jan-17	12-Mar-20
3	Brill	Sep-19	Sep-20
6	Haddenham	Sep-19	Sep-20
7	Marlow	04-Jan-16	Nov-18
8	Olney	Jul-19	Jul-20
9	Stokenchurch	04-Jan-16	Nov-18
11	Beaconsfield	14-Apr-21	12-Apr-22

12	Broughton	26-Mar-20	Mar-20
13	Chesham	07-Aug-17	Nov-18
14	Great Missenden	04-Jan-16	Nov-18
15	High Wycombe	04-Jan-16	Nov-18
16	Newport Pagnell	20-May-15	Apr-17
17	Princes Risborough	04-Jan-16	Nov-18
18	Waddesdon	Jul-19	Jul-20
19	Winslow	Jul-19	Jul-20

Out of sixteen directorates BCPs, we noted that eleven were not reviewed as planned:

#	Directorates	Issue Date	Planned Review Date
1	Finance & Assets (includes Finance, Property, Payroll, Fleet, Procurement)	01-Apr-18	Apr-19
2	Organisational Development	06-Mar-18	05-Jan-22
3	Operational Assurance	04-Jan-16	Nov-18
4	Operational Training	30-Jan-18	Dec-20
5	Buckinghamshire Protection	09-Aug-16	Nov-18
6	Milton Keynes Protection	13-Mar-20	May-21
7	Resource Management Team	27-Jul-16	Jul-20
8	Policy & Resilience	04-Feb-20	Feb-21
9	Technical	28-Jul-20	Jul-21
10	Health & Safety	09-Aug-16	Mar-21
11	Data Intelligence Team	04-Jan-16	Nov-18

There is a risk that critical changes might be missed due to failure to update the BCPs and result in an ultimate failure to recover should an event.

BMKFA should update the BCPs annually for all critical functions or as and when there is a critical change in the process.

Full restructure of business continuity processes – date to be confirmed following investigation of potential options and associated costs and resource requirements (delivery of these by 31 March 2024).

Finding 5: BCP Lessons Learned	Risk Rating	Agreed Management Actions
We noted that the lessons learned were not identified since the BCPs were not tested since 2019. The Authority cannot, therefore, identify the BCP's positive or negative experiences due to failure to perform the BCP testing. The Authority should ensure that lessons learnt are identified once the BCPs are tested to ensure that the organisation doesn't repeat the same mistakes. The outcomes of these tests should be formally documented and identified 'as lessons learnt.	M	**Action:** A full restructure of the Business Continuity Management structures and processes is required to fully meet the recommendations, which would include the development and implementation of a business continuity system that formally records learning and any required actions from learning following exercises and business continuity events. In the meantime, the capture of learning opportunities will be included in the pilot testing programme specified under Finding 3 above. **Officer responsible:** Station Commander Resilience & Business Continuity **Date to be implemented by:** Piloting - 31 March 2024. Full restructure of BCM to be confirmed following investigation of potential options and associated costs and resource requirements (delivery of these by 31 March 2024).
Finding 6: BCP Monitoring and Reporting	**Risk Rating**	**Agreed Management Actions**
While we noted that BCP is discussed at a PMB forum as an overlap as part of risk management reporting, we confirmed that no regular reports regarding business continuity are produced. The Authority should ensure that it is effectively monitoring the business continuity management system and seek assurance that it remains effective and fit for purpose. Consideration should be given to regularly updating various governance forums available at the Authority on current business continuity activities. This could include but not be limited to: • An annual report on the business continuity management system; • Any activation of business continuity plans and the lessons learned; • Outcomes from business continuity tests; and	M	**Action:** A full restructure of Business Continuity Management structures and processes is required to fully meet the recommendations which would include the development and implementation of a reporting system to provide business continuity performance information e.g. number of plans out of review date, number of plans exercised. **Officer responsible:** Station Commander Resilience & Business Continuity

• Outcomes from any dip sampling of business continuity plans. There is an increased risk that an ineffective or inappropriate business continuity system is not identified through regular monitoring and reporting, placing the Authority at risk of being unable to carry out its statutory duties effectively in the event of an incident or emergency.		**Date to be implemented by:** The outcomes of ongoing monitoring of business continuity plan reviews and testing will be reported to PMB on an annual basis (April 24 for first report). Future reporting system development options / proposals 31 March 2024)
Finding 7: ICT Disaster Recovery Plan - Roles and Responsibilities	**Risk Rating**	**Agreed Management Actions**
Upon review of the BMKFA ICT disaster recovery plan, we noted that although there are names and job titles of the individuals with the responsibilities of activating the plan mentioned within the ICT disaster recovery plan, there are no further contact details. Those individuals are the Head of Technology Transformation & PMO, ICT (ICT Manager), and ICT (Service Desk Manager). BMKFA should include the contact numbers of the individuals with the responsibilities of activating the ICT DR Plan within the plan enabling ease of getting contact details in case of a disaster. There is a risk that staff would not know how to contact key staff members in the event of a disaster.	**L**	**Action:** Information to be added to the document on resilience direct. **Officer responsible:** ICT Manager **Date to be implemented by:** 1 March 2023

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	A sound system of governance, risk management and control exist, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited.	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 generally sound system of governance, risk management and control in place. Some issues, non-compliance or scope for improvement were identified which may put at risk the achievement of objectives in the area audited.	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.
Limited	Significant gaps, weaknesses or non-compliance were identified. Improvement is required to the system of governance, risk management and control to effectively manage risks to the achievement of objectives in the area audited.	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.
No Assurance	Immediate action is required to address fundamental gaps, weaknesses or non-compliance identified. The system of governance, risk management and control is inadequate to effectively manage risks to the achievement of objectives in the area audited.	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 actioned. 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 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:
Stuart Gowanlock	Corporate Planning Manager
Suzanne Connolly	Resilience & Business Continuity Manager
Lewis Higgins	ICT Service Desk Manager

The Exit Meeting was attended by:

Name:	Title:
Stuart Gowanlock	Corporate Planning Manager
Lewis Higgins	ICT Service Desk 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

Name:	**Title:**
Stuart Gowanlock	Corporate Planning Manager
Suzanne Connolly	Resilience & Business Continuity Manager
Lewis Higgins	ICT Service Desk Manager
Mark Hemming	Director of Finance and Assets

Final Report as above plus:

Jason Thelwell	Chief Finance Officer
Ernst and Young	External Audit

Audit Control:

Closing Meeting	12 December 2022
Draft Report	31 January 2023
Management Responses	10 February 2023
Final Report	22 February 2023

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

Business Assurance and Risk Management

Pension Fund Administration - FINAL

Auditors

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

Selina Harlock, Audit Manager

Juan Fosco, Audit Manager

Temi Tewogbade, Senior Auditor

Harriet Green, Senior Auditor

Management Summary

Introduction

The Pension Fund Administration audit is being undertaken as part of the 2022/23 Internal Audit plan. The pension administration processes for Buckinghamshire and Milton Keynes Fire Authority (BMKFA) are carried out by an external service provider, West Yorkshire Pension Fund (WYPF). WYPF utilise an internally developed pension system called UPM to manage the pension administration process, maintain member profiles and record invoices for overpayments.

Following a tendering exercise undertaken in October 2015, the Authority moved the administration of the firefighters' pension schemes from Buckinghamshire County Council (as was) to WYPF in January 2016. The contract was awarded for 65 months (5 years and five months) and extended for three years in 2021.

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 for the creation, management and outputs of the Authority's Pension Fund Administration.

- To provide assurance that there are adequate arrangements in place that ensure achievement of the programme goals, effective management and reporting of the progress and risks for all projects being delivered across the Authority.

This will serve as a contribution toward 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

It should be noted that the provider (WYPF) received their audit, and we have received a copy of the audit report. However, we have not placed reliance in that report. The agreed scope of this audit was:

- Policies, Procedures and Training
- System Access, Data Security, and Integrity
- Service Level Agreement with External Customers
- Opt-in/out and Transfers
- Employee and Employer Contributions
- Reconciliations
- Performance Monitoring
- Risk Management and Fraud Risks

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

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
Policies, Procedures and Training	Substantial	0	0	0
System Access, Data Security, and Integrity	Substantial	0	0	0
Service Level Agreement with External Customers	Substantial	0	0	0
Opt-in/out and Transfers	Substantial	0	0	0
Employee and Employer Contributions	Substantial	0	0	0
Reconciliations	Substantial	0	0	0
Performance Monitoring	Substantial	0	0	0
Risk Management and Fraud Risks	Substantial	0	0	1
Total		0	0	1

Appendix 1 defines the grading for each of the conclusions given.

Policies, Procedures and Training

Six policies, procedures, and statements are related to Buckinghamshire's Pension Fund (BPF) Administration. These are:

- The BPF Administering Authority Discretionary Policy,
- BPF Communication Policy Statement,
- BPF Data Improvement Plan,
- BPF Governance Compliance Statement,
- BPF Pension Administration Strategy and Charging Schedule and
- BPF Reporting Breaches of Law Policy.

The LGPS Regulations 2013 and subsequent amendments govern how the pension scheme is administered. We confirmed that all six are available on the Council's website. Following the LGPS Regulations 2013, the administering authorities are required to develop a pension administration strategy to define the following:

- The procedures for liaison between administering authority and participating employers.
- The required performance levels for both the administering authority and participating employers and action to be taken where targets are not met.

We confirmed that the Council developed a Pension Administration Strategy. However, the latest version published on the Council's website is dated July 2020 and updates were made to the LGPS Regulations in 2021. Therefore, the Strategy should be reviewed to reflect any changes and ensure it is up to date. The BMKFA Pensions Officer indicated that the Council administers policies and procedures and that the Fire Authority is not involved in reviewing or updating the policies. Therefore, a recommendation was not raised.

We also confirmed that there are a number of local procedural guidance documents for BMKFA staff to process transactions relating to pension in a correct, complete, and timely manner. This is done via the 'iConnect' system, a secure platform that automates the submission of LGPS pensions data. Process notes are also provided by WYPF for training on calculations, checking data and uploading files to WYPF.

When relevant updates are made to legislation, trends and the service, staff are made aware through intranet articles. During our fieldwork, we confirmed that the most recent communication was relevant to the Annual Benefits Statement (ABS) for 2022, published in September 2022. Also, the Council's team offered a training session and advertised twice on the Authority's intranet. However, there were no opt-ins to the drop-in training.

System Access, Data Security, and Integrity

Pension-related information is pulled from iTrent (the Authority's payroll system). This is then uploaded onto iConnect and sent to the Council concerning pension contributions. The Authority's Pensions Officer indicated that only three staff members have access to iConnect. These are the Pensions Officer, the Payroll Officer at the Authority, and the Council's Pensions System Controller. This was confirmed by reviewing a report listing users and relative system access. We also confirmed that accounts are password protected.

We noted that the iConnect system guidance document does not stipulate the frequency of which passwords must be renewed. The Pensions Officer indicated that iConnect system admin rights (including password changes) sit with the Council. The Fire Authority do not have any control or input on the guidance against

how frequently passwords should be updated. Although we have not raised a finding, the Authority could liaise with the Council's Pensions System Controller to assess whether admin rights could be granted to the Authority to enforce password updates.

Service Level Agreement with External Customers

Following a tendering exercise undertaken in October 2015, the Authority moved the administration of the firefighters' pension schemes from Buckinghamshire County Council (as was) to WYPF in January 2016. The contract was awarded for 65 months and extended for a further three years in 2021, covering May 2021 to May 2024.

A Service Level Agreement (SLA) is in place between the Council and other employers, which runs coterminous with the Council's financial year. This year's commenced on 1 April 2022. The agreement states that 'the 2022 version of the SLA incorporates changes to previous versions, resulting from changes to the LGPS Regulations and internal processes'.

Among others, the SLA includes the following areas:

- New entrants,
- Opt-outs,
- 50/50 section,
- Reduction in Pay,
- Changes,
- Monthly Contributions,
- Year-end Return,
- Additional Contributions,
- Absences,
- Change of Payroll Provider,
- Estimates,
- Leavers and Retirement Death in Service.

Opt-in/out and Transfers

The government requires that all employers provide a workplace pension scheme and automatically enrol employees who meet their criteria. This is called 'automatic enrolment', and a form is not required to enrol the eligible employees on the scheme. However, the employees must sign an opt-out form to be removed from the scheme.

At the Authority, the Payroll team automatically enrols all new joiners eligible for the pension scheme. We obtained a report listing all staff at the FA and their respective pension status. This report lists all staff at the Authority and identifies those who opted out (more details below) and those who are not eligible for auto-enrolment, such as those earning less than £10k per annum or agency staff.

We confirmed that the remaining staff is listed in the report with detailed pension IDs. Additionally, there is a three-year auto-enrolment requirement for all eligible staff members to be re-enrolled into the pension scheme. BMKFA are undergoing an auto-enrolment in November 2022, per the three-year requirement. The

previous auto-enrolment was undertaken in November 2019. As part of this previous exercise, we obtained evidence of an email sent to a staff member in December 2019 informing them of re-enrolment into the pension scheme.

Individuals who meet the criteria for auto-enrolment can opt out of the scheme by completing the opt-out form. We obtained a report of all individuals who opted out of the pension scheme as of October 2022. There were 10 instances in total. From this, we selected a sample of five employees and confirmed evidence was retained on file of the completed opt-out form. We additionally confirmed through a review of payslips that they opted out promptly, and four employees paid no contributions in the following month.

One of the individuals tested opted out in June 2022 and the request was processed in July. As the employee was in the scheme for under three months, the Authority's Payroll Team refunded their pension contributions, not WYPF. This was evidenced on their payslip as back pay. I-Trent does not have this option on the system, so the Payroll team refunded the contribution using a different function.

The Pensions Officer indicated that, apart from the opt-in and opting-out of staff members, all other administration is undertaken by WYPF. Therefore, there is no specific report of all transfers in and out and adjustments for the last 12 months.

Employee and Employer Contributions

Reconciliations are undertaken monthly by the Pensions Team at the Authority between the contributions calculated from iConnect and the payment request from WYPF.

We selected a random sample of 12 employees from November 2021 to April 2022. For each case, we confirmed that the employee contribution calculated from iConnect reconciled with the amount paid by the employee in their monthly payslip.

Additionally, we confirmed that the contribution amounts for each employee sampled are in line with the SLA LGPS Contribution table percentages.

Reconciliations

The BMKFA's Pensions Team also undertake monthly reconciliations between iConnect reports and the amounts required from LGPS. Any differences are noted and investigated.

We obtained evidence of the reconciliations completed between November 2021 to April 2022. We confirmed that reconciliations and spot checks are undertaken monthly. iConnect reports from February, April and May 2022 all reconcile with the amounts requested from LGPS.

The March, June and July 2022 reports pulled from iConnect did not reconcile with the amounts requested from LGPS. Differences between the employees' main contribution, employer's contribution and pensionable pay were highlighted and investigated within the iConnect reports with no apparent subsequent issues.

Performance Monitoring

Under the Service level agreement between BCC and WYPF, it is stated that the performance of the service shall be measured against obligations, standards, targets and benchmarks relevant to the provision of service.

Within two months before the beginning of each Contract year, WYPF will prepare an annual contract review containing an analysis of the service provided and an action plan setting out future measures in response to the review. The BMKFA Fire Fighters Local Pension Board meet monthly to discuss WYPF performance against KPIs, declarations of interest, risk management/register updates and actions from the action log.

BMKFA's Local Pension Board meeting minutes from March 2022 to August 2022 were obtained. It was noted that KPIs for WYPF are reviewed at every meeting.

The meeting minutes were reviewed alongside monthly reports provided by WYPF, which list the specific KPIs and the number of targets met/not met. There were issues in July 2022 where Pension Set Up/Payment of Lump Sum, Retirement Actual and Deferred Benefits Set Up on Leaving did not reach their targets. This was highlighted in the following Pension Board meeting. However, we noted a lack of scrutiny around discussions relevant to the failed KPIs in the minutes reviewed. We were informed that discussions concerning improving KPIs occur. However, the minutes viewed do not evidence this. **(Recommendation 1)**

Risk Management and Fraud Risks

The Overview and Audit Committee on 20 July 2022 presented the corporate risk register to be reviewed and approved. Before this, the Corporate Risk Register was last reviewed by the Overview and Audit Committee at its 16 March 2022 meeting. Since then, it has been subject to review by the Performance Monitoring Board (PMB), at which all the directorate and departmental risk registers were reviewed, and by SMB at its monthly meetings.

Also, Lead Members were consulted during the evaluation process for risks falling within their portfolios of responsibility. The risk register was updated to reflect ongoing monitoring of staffing and financial risks associated with Court rulings concerning firefighter pension schemes.

The risk of the potential impact on staff retirement profile, resourcing to implement changes, and financial impacts due to the Court of appeal ruling have been identified. There are two risk owners, the Lead Member for Finance and Assets and the Information Security & IT Director for Finance & Assets.

The Current treatment is to factor the potential impacts on costs into the future Medium-Term Financial Planning Process and recruitment of dedicated specialist resources to evaluate requirements arising from the Court of Appeal ruling and implement necessary administrative changes. The consequences of the risk being untreated have been documented, and a risk score has been assigned. Compared to the former risk score, the score has decreased in light of the measures taken. Comments, updates and further treatment proposed have been illustrated within the register.

Addition of Starters and Removal of Leavers on the pension system

We selected a sample of eleven starters, for April, May, and June 2022 and reviewed screenshots from the pension portal and confirmed that they had been enrolled on the pension system.

We selected a sample of five leavers to confirm that in each instance a leaver form had been signed off to process their departure and we noted the following:

- We were provided with evidence to confirm that in two cases the leavers had leaver forms completed by Pension Officer.

- Management indicated that in one case the leaver was not entitled to be in the pension scheme as they were on a casual contract.

- In the remaining two cases, management indicated that the employees are part of the Local Government Pension Scheme (LGPS), so no leaver forms are required by the fund. A leaving date on the monthly return is all the Bucks LGPS fund requires. We reviewed the monthly returns and noted that the payroll period end date was 30 April 2022 for these employees.

Table 2: Detailed Audit Findings and Management Action Plan

Finding 1: Performance Monitoring/KPIs	Risk Rating	Agreed Management Actions
We reviewed the controls around performance monitoring of the service provided by WYPF. We noted that WYPF provides monthly updates to the Authority, and KPIs and performance are discussed as a standing item at each Pension Board meeting. There were issues in July 2022 where Pension Set Up/Payment of Lump Sum, Retirement Actual and Deferred Benefits Set Up on Leaving did not reach their targets. This was highlighted in the following Pension Board meeting. However, there is a lack of evidence concerning scrutiny and challenge within minutes. In addition, no review of whether KPIs are still fit for purpose or whether they should be amended has taken place. If KPIs are not scrutinised in detail, and this is documented in minutes, there is a risk that any underperformance is not being rectified in time. This could lead to continuous poor performance, which could impact the Authority's reputation and/or create financial loss.	L	A review of the current KPI's with WYPF at the Pension Board to ensure they are fit for purpose. These KPI's will be scrutinised and challenged by the board and minutes documented. **Officer responsible:** Pension Officer (Emma Hamilton) **Date to be implemented by:** 31 December 2023

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	A sound system of governance, risk management and control exist, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited.	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 generally sound system of governance, risk management and control in place. Some issues, non-compliance or scope for improvement were identified which may put at risk the achievement of objectives in the area audited.	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.
Limited	Significant gaps, weaknesses or non-compliance were identified. Improvement is required to the system of governance, risk management and control to effectively manage risks to the achievement of objectives in the area audited.	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.
No Assurance	Immediate action is required to address fundamental gaps, weaknesses or non-compliance identified. The system of governance, risk management and control is inadequate to effectively manage risks to the achievement of objectives in the area audited.	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 actioned. 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 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)
Laura Taylor	Principal Accountant (Management Accounting)
Emma Hamilton	Pensions Officer

The Exit Meeting was attended by:

Name:	Title:
Asif Hussain	Deputy Director of Finance and Assets
Emma Hamilton	Pensions Officer

We 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
Laura Taylor	Principal Accountant (Management Accounting)
Marcus Hussey	Principal Accountant (Technical Accounting)

Final Report as above plus:

Jason Thelwell	Chief Fire Officer
Ernst and Young	External Audit

Audit Control:

Closing Meeting	14 October 2022
Draft Report	9 December 2022
Management Responses	7 February 2023
Final Report	8 February 2023

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

HR Payroll Process Review

February 2023

Introduction

This report provides a summary of the Human Resources (HR) Payroll Process Review, which evaluated the processes relating to data processed by the HR and Payroll teams and also included inputs from other teams and systems, such as operational resource management data from Fire Service Rota. We conducted walkthroughs with relevant personnel who process HR and Payroll data to understand the current processes in place, which has allowed us to map the systems and processes in a "swim-lane" format, highlighting individual responsibilities.

Reviews were conducted for each process that results in a data entry on iTrent, the roles and responsibilities for these processes, as well as for controls relating to transfer of data between systems.

The slides for each process provide an overview of the control gaps that we observed. Comprehensive process maps are linked to each process summary and through these links the detailed process maps can be viewed.

In our review of the HR and Payroll control framework, we have also considered the findings raised in previous internal audit reviews of HR, Payroll and Resource Management. We have evaluated the progress made to implement these actions.

Contents	Slide
Executive Summary	3
Key iTrent System functions	4
Process Overview	6
Starters	7
Leavers	8
Positional Moves	9
ITrent Users	10

Executive Summary

The purpose of this assurance review was to have complete visibility of all processes requiring input from both the Payroll and HR teams and to ensure that HR and Payroll controls are adequate. This included an evaluation of all starters, leavers and changes processes, along with discovery of any additional processes, and their input into iTrent (the Payroll system) and, where relevant, Integra (the Finance system).

The 2020/21 Core Financial Controls Audit and 2019/20 Core Financial Controls Audit both identified weaknesses in the system of internal control for Payroll. The 2020/21 Core Financial Controls Audit included a finding in respect of the flow of information from HR to Payroll during the Leaver and Change of Role processes, noting that the relevant teams would benefit from end to end process mapping 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.

The HR/Payroll Process Review follows on from the following previous internal audit reviews :

- **2021/22 HR People Management audit** – two medium priority findings relating to processes that involve both HR and Payroll were raised. The area conclusion for Starters, Leavers and Movers was **Reasonable.** The overall audit opinion was **Reasonable**.
- **2020/21 Core Financial Controls audit** – two medium priority findings relating to Payroll were raised. The area conclusion for Payroll was **Reasonable**. The overall audit opinion was **Substantial**.
- **2019/20 Core Financial Controls audit** – one low priority finding relating to Payroll was raised. The area conclusion for Payroll was **Substantial.** The overall audit opinion was **Substantial**.
- **2017/18 Core Financial Controls audit** – one medium priority finding was raised. The area conclusion for Payroll was **Reasonable.** The overall audit opinion was **Substantial**.

The table below provides a summary of all the findings raised and their implementation status:

Internal Audit Title and Year	Number of Payroll/HR process related findings	Medium Priority			Low Priority		
		Implemented	Partially Implemented	Not Implemented	Implemented	Partially Implemented	Not Implemented
HR People Management 2021/22	2	1	-	-	1	-	-
Core Financial Controls 2020/21	2	1	1	-	-	-	-
Core Financial Controls 2019/20	1	-	-	-	1	-	-
Core Financial Controls 2017/18	1	1	-	-	-	-	-
Total	4	2	1	-	1	-	-

Key iTrent system functions

Recruitment

- The iTrent Recruitment module includes:
    - Authorisation/approval to recruit
    - Determine advertising strategy
    - Place advertisement with chosen media
    - Receive and progress applications
    - Identify, offer and appoint suitable applicant into the organisation.
- Trigger for the recruitment process is the identification of a recruitment requirement, which may be as a result of a leaver within the organisation or the creation of a new position.
- Match and Gap - compares the attributes of an individual an applicant with the requirements of a vacancy. Compares items associated with the Profile – Qualifications, Qualification statuses, Skills, Skill sets, Memberships and Checks.

Sickness absence reporting

- Recorded by employees via the Payroll and HR Employee Self Service (ESS) Portal.
- Approved/administered by managers via the People Manager portal
- Reports on absence history can be generated for individual employees or by team/organisation.
- Sickness absence data for operational staff is recorded via Fire Service Rota, the Fire Authority's Resource Management system.

Key iTrent system functions cntd.

Payroll

- Allows complex payroll scenarios to be achieved through user-defined calculation rules. Automated retrospection functionality allows for payroll reversals that are easy to manage.
- Interactive payslips.
- Payroll cut-offs automatically decide which requests are processed in which pay period.
- Automated electronic payments to HMRC and other third parties.
- Flexible two-stage bank detail verification process for employees, through integration with GB Group (GBG) identity verification software, helps protect the Fire Authority against payroll fraud and reduces the time spent chasing payment reclaims.

Expenses

- Claimed by employees via the Payroll and HR ESS Portal.

People Manager

- Provides managers with access to a range of information about their staff.

Process Overview

The below diagram provides an overview of the different HR and Payroll processes, the relevant systems and the associated volumes of transactions for the period between December 21 to November 22 for each process.

Comments / Limitations on data:

- Figures were retrieved from reports generated from iTrent, the Fire Authority's Payroll system.
- Data for Starters, Leavers, temporary changes and permanent changes (included as Positional Moves) is held on the employee's ePRF (electronic Personnel Record File) and on iTrent.
- Data for operational staff, including that for absences, availability and positional moves, is held on Fire Service Rota (the Fire Authority's planning and scheduling system).

HR/Payroll Processes

Recruitment — 37 (new roles created)

Starters — 86

Positional Moves — 240

Leavers — 974
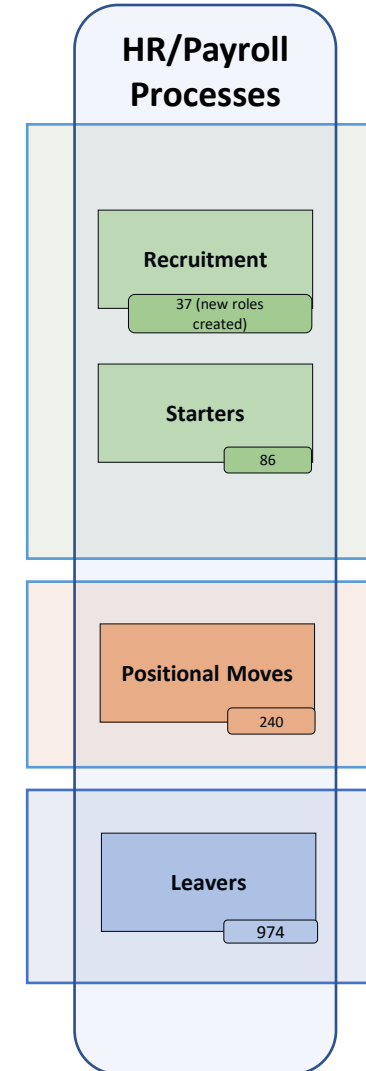
Starters

Summary – New Starters are added to iTrent by HR following the recruitment process, with documents added to the electronic Personnel Record File (ePRF) as they are received and as the New Starter process progresses. Any remaining payroll information is collected and entered by Payroll, with inputs checked and relevant calculations completed.

Interview List – Jackie Vere-White (Payroll and Benefits Manager); Anne Stunell (Head of Human Resources); Carly Humphrey (HR Operations Manager).

Control Risk Observations and Recommendations

Area	Observations	Previously raised?	Risk Rating	Recommendation
Starter Checklist	Comprehensive New Starter checklists are in place to record inputs and checks completed by both the HR and Payroll teams when setting up a new starter. Review of the HR and Payroll checklists established that separate checklists are completed by the HR and Payroll teams and that each team does not have sight of the other team's checklist. The following tasks and document checks were found to be duplicated across both checklists: • Offer letter and signed contract; • Personal Details form; • HMRC New Starter Declaration; • Right to work check; and • Entry of pay and contract information into iTrent. Additionally, discussion with the Payroll Manager established that Pension-related inputs are sometimes completed by HR, although this is the responsibility of the Payroll and Benefits team. Where such tasks are completed by the team not usually responsible for completion of the task, the other team is not notified.	No	M	Review tasks listed on both the HR Starter checklist and Payroll Starter checklist and ensure they are not duplicated across the two functions but that sufficient checks remain in place. Produce a new Starter checklist that is accessed by both HR and Payroll and includes all tasks related to processing Starters for both functions. **Management Action/ Response** The HR Operations Manager and Payroll and Benefits Manager (and teams) to review the checklists and process maps/flow diagrams, with a view to combining them into one document.

(**) – shows the process step in question – see map for further details

Leavers

Summary – Leavers are actioned by HR when notification is received that an employee is leaving. Payroll tasks are workflowed to Payroll for them to action before the final payslip is issued.
Interview List – Jackie Vere-White (Payroll and Benefits Manager); Anne Stunell (Head of Human Resources); Noma Magutshwa (HR Officer - Recruitment and Operations).

Control Risk Observations and Recommendations

Area	Observations	Previously raised?	Risk Rating	Recommendation
Leaver Checklist	Leaver checklists are in place to record actions and checks completed by both the HR and Payroll teams when processing employees as leavers. However, it was noted that HR and the Payroll and Benefits team were working from separate checklists and did not have sight of actions completed by the other team. Whilst there were no apparent duplications in tasks, or discrepancies over the responsibility for actions between the checklists, it would benefit the Leavers process to have a Leaver processing checklist that can be accessed by both teams so that relevant officers are aware that data has been input and checked by other officers involved in the process, to enable them to continue with subsequent process steps and to avoid any duplication or missed steps.	No	L	Review tasks listed on both the HR Leaver checklist and Payroll Leaver checklist and ensure they are not duplicated across teams but that sufficient checks remain in place. Produce a new Leaver checklist that is accessed by both HR and Payroll and includes all tasks related to processing Leavers for both functions. **Management Action/ Response** The HR Operations Manager and Payroll and Benefits Manager (and teams) to review the checklists and process maps/flow diagrams, with a view to combining them into one document.

(**) – shows the process step in question – see map for further details

Positional Moves

Summary – When notification is received by HR of upcoming changes, a Change Control form is completed by the employee's manager or Learning and Development team. This is then processed by HR, with the involvement of Payroll if a change to Payroll is required. There are 12 types of changes submitted via Change Control forms.
Interview List – Jackie Vere-White (Payroll and Benefits Manager); Anne Stunell (Head of Human Resources)

Control Risk Observations and Recommendations

No control risk issues were noted in respect of the process positional moves. See process map for controls identified as part of the process review.

iTrent Users

Summary – The iTrent system has a total of 973 users (including users of the Employee Self Service module). This includes:

- •154 users with People Manager access
- •8 Payroll BAU users
- •8 HR BAU users

No control risk issues were noted in respect of iTrent users and user access.

Appendix A - Follow-Up Findings

Implementation status of findings raised and management actions agreed during the 2021/22 internal audit of HR People Management and the 2020/21 internal audit of Core Financial Controls.

HR People Management 2021/22

Report Ref No. 1	Title: Starters, Leavers and Movers - New Starters	Priority of finding: M	Status: Implemented
Original Audit Finding		**Management Comments & Action Plan**	
Examination of a sample of 20 new starters at the Fire Authority between January 2021 and July 2021 found: • One case where no contract, offer letter, checklist, references or ID were provided. • Five cases where no references were provided. In all five cases references were requested but either not received or not available on the personnel file as of the audit. In seven further cases, only one reference was provided. Discussion noted that one was an apprentice, with apprentices only having one reference due to a lack of prior experience, and one was an agency employee for which a different process is in place. Therefore, five of the seven cases were exceptions. • Two cases where no medical questionnaire was held on file. • Two cases where the starter checklist was not fully completed.		HR to communicate to the organisation what is expected from them in order to process new starters according to the agreed process. HR to review the process notes and ensure completion of new starter checklist.	
Follow Up Evaluation		**Further Recommendation**	
HR coach managers through the processes as part of the support they provide on recruitment and selection. The process notes have been and are reviewed on an ongoing basis, in line with legislation and best practice. The checklist is used for every new starter and stored on the employees personal file once complete, as per the agreed process.		N/A	

Follow-Up Findings

Report Ref No. 4	Title: System Transactions and Records – Leaver access not removed	Priority of finding: L	Status: Implemented
Original Audit Finding		**Management Comments & Action Plan**	
Examination of a sample of 20 employees whose information changed between January and July 2021 found: • In one case, the instruction to make the change was received on the effective date. In this case it was entered on iTrent four days later. Whilst the other five changes applied retrospectively were deemed to be outside the control of HR, in this case HR was deemed to be partially responsible for the delay. • Two cases where there was no Change Control Form. Discussion established that these roles were both from a recruitment process. A Change Control Form is not a requirement for these as HR are involved in the interview processes and therefore know the details of the transfers. Some managers do provide Change Control Forms, but they are not required as approval is already received. However, there is another similar example where a Change Control Form was provided. Discussion with the Senior Administrator established that some operational roles have allowances that require the Appointments Board to provide additional approval on a change control form. However, where there are such variations in the process, they should be identified in the process notes.		HR to communicate to the organisation what is expected from them in order to process changes according to the agreed process. HR to review the process notes and conclude the new change control form consultation and relaunch the form.	
Follow Up Evaluation		**Further Recommendation**	
HR coach managers through the processes as part of the support they provide on changes and leavers. The process notes have been and are reviewed on an ongoing basis, in line with legislation and best practice. Change control form consultation undertaken and new electronic form launched, utilised by 95% of people, the others have used a business case as an alternative or the old form and told about the process for the future. HR welcome ongoing feedback on the form, and continue to make amendments as necessary.		N/A	

Follow-Up Findings

Core Financial Controls 2020/21

Report Ref No. 1	Title: Payroll–Authorisation of CPD payments	Priority of finding: M	Status: Implemented
Original Audit Finding		**Management Comments & Action Plan**	
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.		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.	
Follow Up Evaluation		**Further Recommendation**	
Effective from April 2021 there has been a change in process that CPD is awarded to all Operational Firefighters automatically at the point that they achieve Competency. A Procedure for CPD has been published which references this, the process and procedural guidance note for CPD is the responsibility of our Organisational Development Team. The change from Development to Competency is advised by our Organisational development Team who validate the completion of Development Folders for all ranks. The OD team will complete a Change Control Form detailing the move from Development to Competent, this will prompt a change in pay scale and also the application of CPD. This is approved by the Budget Holding Station Commander and changes are then processed by Payroll.		N/A	

Follow-Up Findings

Report Ref No. 2	Title: Payroll–Flow of information from HR to Payroll during Leaver and Change of Role processes	Priority of finding: M	Status: Implemented

Original Audit Finding	Management Comments & Action Plan
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.	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.

Follow Up Evaluation	Further Recommendation
End to end process mapping completed and recommendations have been raised with the services involved.	N/A

Follow-Up Findings

Core Financial Controls 2019/20

Report Ref No. 3	Title: Payroll – Voluntary deductions	Priority of finding: L	Status: 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. Deductions should be authorised by the employee prior to 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 Drawer 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		**Further Recommendation**	
A review of Prize Draw deductions was undertaken in March 2021 to re-obtain approval for the Prize Draw deduction and the deduction was relaunched for the 2021/22 financial year.		N/A	