LEICESTERSHIRE
FIRE and RESCUE SERVICE

Status of Report: **Public** **Agenda Item:** **7**

Meeting: **Overview and Scrutiny Committee**

Date: **3rd September 2014**

Subject: **Internal Audit Reports 2013-14**

Report by: **The Treasurer**

Author: **Adam Stretton (Head of Finance)**

For: **Discussion**

1. Purpose

Under the Combined Fire Authority's (CFA) Financial Procedure Rules the Treasurer (the Director of Finance and Corporate Services) is responsible for arranging a continuous internal audit of the CFA's accounts. This report brings to the attention of the Overview and Scrutiny Committee a number of Internal Audit reports based upon the 2013/14 Annual Internal Audit Plan.

2. Executive Summary

2.1 Based on the testing undertaken for the Day Crewing Plus Duty System and the Joint Audit 2013/14 Part two, it was determined that **full assurance** can be given with no recommendations made.

2.2 Based on the testing undertaken for Duplicate Payments, Budget Monitoring, Joint Audit on Key ICT Controls and the Payroll 2013/14 Final Audit, **substantial assurance** was given that the internal controls tested were operating adequately as intended to reduce exposure to those associated risks currently material to the system's objectives. Three recommendations were made requiring management action for the Duplicate Payments; three recommendations made for Budget Monitoring; fourteen recommendations for the Joint Audit review of Key ICT Controls; and two recommendations made for the Payroll 2013/14 Final Audit.

2.3 For the testing undertaken for Risk Management, it is acknowledged that transitional arrangements are in place. As such, a level of **reasonable assurance** is given with a future target level of substantial assurance to be achieved during 2014/15.

2.4 Following the identification of the submission of duplicate reimbursement claims, the Director of Finance and Corporate Services requested that Internal Audit examine the revised processes put in place. Three recommendations have been made.

3. Report Detail

3.1 All Internal Audit reports are prepared on an exception basis. Where items have not been reported on, based on the sample examined, the CFA can draw confidence that controls are operating satisfactorily. The full list of testing undertaken within each Audit can be supplied upon request.

Day Crewing Plus Duty System

3.2 As a part of the 2013/14 Internal Audit Plan, a review of the management of the roll out of the Day Crewing Plus (DCP) Duty System was undertaken.

3.3 The Internal Audit control objectives were to provide assurances to management that the lessons learned from the internal review of the Day Crewing Duty System and shift pattern at Melton are taken forward and that risk is being mitigated within the roll out of DCP.

3.4 Full details of the audit can be found in **Appendix 1**. Based on the answers provided during the audit and the sample testing undertaken, **full assurance** can be given that the internal controls in place to reduce exposure to those agreed risks currently material to the system's objectives are adequate and are being managed effectively. No recommendations have been made to improve the system's controls and no material risk exposure has been identified.

Joint Audit 2013/14 Part Two

3.5 As a part of the 2013/14 Internal Audit Plan, a review of the systems and procedures in place for the reconciliation of key ledger, payroll control and suspense accounts was undertaken. Testing covered the period of February 2014 as agreed between Internal and External Audit.

3.6 The Internal Audit control objectives were to ensure that key reconciliations and other agreed processes were undertaken accurately and promptly in the following areas:

- Bank Reconciliations
- Receivable and Payables Control Accounts
- Opening and Closing Balances
- Salaries Reconciliations

3.7 Full details of the audit can be found in **Appendix 2**. Based on the answers provided during the audit and the testing undertaken, **full assurance** can be given that the internal controls in place to reduce exposure to those agreed risks currently material to the system's objectives are adequate and being managed effectively. No recommendations have been made to improve the governance arrangements and no material risk exposure has been identified. This replicates the outcome of the Joint Audit Part One.

Duplicate Payments

3.8 A data matching exercise to identify duplicate payments was undertaken as part of the 2013/14 Internal Audit Plan. This included payments made direct through the Agresso system and those made by Procurement and Credit Card and payments made by Direct Debit.

3.9 Internal Audit considered the overall control objective was to provide assurance to management that there are procedures in place to prevent duplicate payments where at all possible, but also to detect and take corrective action if any have been made.

3.10 Full details of the audit can be found in **Appendix 3**. Based on the answers provided during the audit and the testing undertaken, **substantial assurance** can be given that the internal controls in place to reduce exposure to those agreed risks currently material to the system's objectives are adequate and are being managed effectively. Three recommendations have been made and the management responses to them are found in the Appendix. None of the recommendations have a "high importance" rating signifying a particularly serious control weakness has been identified.

Budget Monitoring

3.11 A review of revenue budget monitoring process was undertaken as part of the 2013/14 Internal Audit Plan.

3.12 The Internal Audit control objectives were to ensure that controls in place to monitor the budget are robust.

3.13 Full details of the audit can be found in **Appendix 4**. Based on the answers provided during the audit and the testing undertaken, **substantial assurance** can be given that the internal controls in place to reduce exposure to those agreed risks currently material to the system's objectives are adequate and are being managed effectively. Three recommendations have been made and the management responses to them are found in the Appendix. None of the recommendations have a "high importance" rating signifying a particularly serious control weakness has been identified.

Joint Audit – Key ICT Controls

3.14 A review of the ICT Controls in operation for the period 1st April 2013 to 31st March 2014 was undertaken as part of the 2013/14 Internal Audit Plan. This work is carried out in accordance with the guidance of the External Auditor, PricewaterhouseCoopers (PwC), as part of the joint audit.

3.15 The Internal Audit control objectives are to ensure that the fourteen key ICT controls included in the review (found in **Appendix 5** as Appendix 1) are operating effectively and efficiently. The work principally referred to Network systems and the Agresso Financial System

3.16 Full details of the audit can be found in **Appendix 5**. Based on the answers provided during the audit and the testing undertaken, **substantial assurance** can be given

that the internal controls in place to reduce exposure to those agreed risks currently material to the system's objectives are adequate and are being managed effectively Fourteen recommendations have been made and the management responses to them are found in the Appendix. None of the recommendations have a "high importance" rating signifying a particularly serious control weakness has been identified.

Joint Audit 2013-14 Part Two

3.17 A review of the procedures in place for administering starters, leavers, variations to pay including deductions relating to employees and pensioners was undertaken as part of the 2013/14 Internal Audit Plan. This audit assists PwC in their annual assessment of the likelihood of material misstatement in the CFA's financial accounts. At the start of 2013/14 financial year the CFA employed just over 859 operational and non-operational staff. The budgeted figures for payroll laid down in the Medium Term Financial Strategy were just under £28.6 million. The Human Resources (HR) and Finance sections are responsible for making sure all data is current and up to date. This information is then forwarded to East Midlands Shared Services (EMSS) Payroll section for inputting onto the payroll system and subsequent payment. This audit was the second review in the year and covered the period December 2013 to March 2014.

3.18 The Internal Audit control objectives were that:

- All new members of staff are bona-fide and are paid at the correct rate from the correct date.
- All leavers are paid up to the correct date and all relevant expenses and advances are recovered.
- All variations to pay have appropriate authorisation and for the correct amount.
- Deductions from pay are accurate and supporting documentation retained.

3.19 Full details of the audit can be found in **Appendix 6**. Based on the answers provided during the audit and the testing undertaken, **substantial assurance** can be given that the internal controls in place to reduce exposure to those agreed risks currently material to the system's objectives are adequate and are being managed effectively. This replicates the findings from the Payroll Audit Part One. Two recommendations have been made and the management responses to them are found in the Appendix. None of the recommendations have a "high importance" rating signifying a particularly serious control weakness has been identified.

Risk Management

3.20 A review of the risk management framework was undertaken as part of the 2013/14 Internal Audit Plan.

3.21 The Internal Audit control objective was to provide assurance that the risk management framework (Corporate Risk Register) is effective in assisting the CFA achieve its objectives.

3.22 Full details of the audit can be found in **Appendix 7**. Based on the answers provided during the audit and the testing undertaken, **reasonable assurance** can be given that the internal controls in place to reduce exposure to those agreed risks currently material to the system's objectives are adequate and are being managed effectively. This outcome is in acknowledgement that action is being undertaken to implement a new Risk Management Procedure. The recommendations made include fundamental areas to be considered for incorporation into any revised framework. None of the recommendations have a "high importance" rating signifying a particularly serious control weakness has been identified.

3.23 Internal Audit will test the implementation of the new Risk Management Procedure in 2014/15 to ensure controls are operating satisfactorily.

Duplicate Training Claims

3.24 Following receipt of information that duplicate training claims had been submitted, the Director of Finance and Corporate Resources requested Internal Audit to examine the revised processes in place to enable Retained Firefighters to claim reimbursement for loss of earnings following attendance at training courses.

3.25 The scope of the audit was to review:

- How the duplicate claims were identified.
- Whether weaknesses are apparent in the use of either the FireWatch and/or the Oracle HR system for claiming training expenses.
- Examination of preventative and detective controls and an assessment of whether key internal controls failed.
- Safeguards in place to prevent similar occurrences and methods used to communicate this within the organisation.
- Whether revised procedures would be likely to prevent this happening again.
- What steps have been taken to investigate the possibility of other such occurrences and provide an opinion on the adequacy of those.
- Ascertain if there are any weaknesses and/or system vulnerabilities in Oracle HR in relation to the processing of training claims.

3.26 Full details of the audit and key findings can be found in **Appendix 8**. The report makes three recommendations for action by the Finance section and the Training Department.

4. Report Implications / Impact

Legal (including crime and disorder)

None.

4.2 ***Financial (including value for money, benefits and efficiencies)***

These are included in the main body of the report.

4.3 ***Risk (including corporate and operational, health and safety and any impact on the continuity of service delivery)***

Internal Audit provides reassurance that effective internal control procedures are in place. Internal Audit reports are used to inform the Treasurer and the Chief Fire and Rescue Officer of the detailed findings of the audit and highlight actions that are required to safeguard the CFA's interests.

4.4 ***Staff, Service Users and Stakeholders (including the Equality Impact Assessment)***

None.

4.5 ***Environmental***

None.

4.6 ***Impact upon Our Plan Objectives***

The CFA's Strategic Objective 4 is the attainment of efficiency and the provision of a value for money service. The provision of internal audit assists both effective and efficient management and good corporate governance. It also externally validates the CFA's progress in this area.

5. Recommendations

The Overview and Scrutiny Committee is asked to note the Internal Audit Reports detailed in Section 3 and listed as Appendices 1 – 8.

6. Background Papers

Internal Audit Plan 2013/14 (Overview and Scrutiny Committee Report - 13th March 2013)

7. Appendices

1. Day Crewing Plus Duty System
2. Joint Audit 2013/14 Part Two
3. Duplicate Payments
4. Budget Monitoring
5. Joint Audit – Key ICT Controls
6. Payroll 2013/14 Final Audit

7. Risk Management
8. Duplicate Training Claims

Appendix 1

Internal Audit Report

Leicestershire County Council
Leicestershire Fire & Rescue Service
Day Crewing Plus Duty System
March 2014

KEY PERSONNEL	
Lynn Woolhouse	Auditor
Matt Davis	Audit Manager
Neil Jones	Head of Internal Audit Service

INTERNAL AUDIT REPORT

LEICESTERSHIRE FIRE & RESCUE SERVICE

DAY CREWING PLUS DUTY SYSTEM

MARCH 2014

1 INTRODUCTION

1.1 A review of the management of the roll out of the day crewing plus duty system was undertaken as part of the 2013/14 LFRS Internal Audit Plan.

2 AUDIT OBJECTIVES

2.1 We consider the control objectives is to provide assurances to management that lessons learned from the internal review of the 'Day crewing' duty system and shift pattern at Melton are taken forward and that risk is being mitigated within the roll out of day crew plus.

2.2 Specific exclusions to the work undertaken are:

- All risks associated with Day Crewing Plus have in fact been identified
- Linkage between the risks raised and the Corporate Risk Management Process *(a separate audit in respect of the Corporate Risk Management process is currently being undertaken)*

3 KEY FINDINGS AND RECOMMENDATIONS

3.1 We have no findings which merit a recommendation.

4 CONCLUSION

4.1 The issues highlighted in the Melton Day Crew post project report have been taken into consideration and, where applicable, have been included in the risks and issues log maintained for the Operational Improvement Project.

4.2 The risks and issues log contains 25 perceived risks directly associated with the introduction of the day crew plus duty system. For each risk stated there is a control measure and lists actions taken.

4.3 At the time of the review, only 5 risks remain open 2 of which have red RAG ratings. Both of these risks are associated with the development of the Castle Donington site which has only recently received approval from Senior Management Team to recommence.

4.4 From our review we were able to ascertain that there is a robust governance process in respect of risks and issues identified with evidence of them being discussed at both the Senior Management Team and at the Overview and Scrutiny Committee (OSC). Furthermore, the minutes of discussions at OSC are also presented to the Combined Fire Authority resulting in transparency throughout the risk management process.

5 OPINION

Based on the answers provided during the audit, testing undertaken and specific exclusions to coverage detailed in 2.2 above, **full assurance** can be given that the internal controls in place to reduce exposure to those agreed risks currently material to the system's objectives are adequate and are being managed effectively.

Appendix 2

Internal Audit Report

Leicestershire Fire and Rescue Service
Joint Audit 2013-14
July 2014

KEY PERSONNEL	
Dilashani Fathers	**Assistant Auditor**
Helen Moran	**Senior Auditor**
Matt Davis	**Audit Manager**

DRAFT INTERNAL AUDIT REPORT
LFRS
JOINT AUDIT PART TWO 2013-14
JULY 2014

1 INTRODUCTION

The 2013-14 Joint Audit with PWC has been undertaken. Further detail as to the background to the audit can be seen in the Terms of Engagement (TOE) as issued to Adam Stretton, Head of Finance in December 2013. This shows the risks, scope and also the methodology adopted to undertake the audit.

2 AUDIT OBJECTIVE

The control objective for this audit was to undertake the testing agreed with PWC and report our findings as appropriate. Period eleven was reviewed in detail for all of the payroll reconciliations. This was different to the scope within the TOE and was agreed with PWC prior to the start of the audit.

3 KEY FINDINGS AND RECOMMENDATIONS

We have no findings which merited a recommendation, as controls were found to be operating satisfactorily in all the areas examined. The full details of testing undertaken can be supplied on request.

4 CONCLUSION

All key payroll reconciliations were being accurately and promptly completed and all adjustments were valid and agreed to supporting documentation. In addition the non-payroll reconciliations were promptly completed. There were no large value old adjustments included in the reconciliations reviewed.

5 OPINION

Based on the answers provided during the audit and the sample testing undertaken, **full assurance** can be given that the internal controls in place to reduce exposure to those agreed risks currently material to the system's objectives are adequate and are being managed effectively.

No recommendations have been made to improve the system's controls and no material risk exposure has been identified.

Appendix 3

Internal Audit Report

Leicestershire Fire & Rescue Service
Duplicate Payments

March 2014

KEY PERSONNEL	
Anita Ryder	**Auditor**
Matt Davis	**Auditor Manager**
Neil Jones	**Head of Internal Audit Service**

INTERNAL AUDIT REPORT

LEICESTERSHIRE FIRE & RESCUE SERVICE

DUPLICATE PAYMENTS

MARCH 2014

1 INTRODUCTION

1.1 As part of the 2013/14 audit plan we have undertaken a data-matching exercise to identify duplicate payments.

1.2 The value of invoices processed via Agresso for 2012/13 totalled £23m.

There are two invoice processes;

- Purchase Order Invoice where the invoice is matched to the order
- Supplier Order Invoice where there is no order therefore no matching takes place

1.3 Furthermore, there are two other electronic ways currently in use to make a payment:

- A bankline transfer from the general business account *(number ending 9318)*
- A direct debit payment from the above account

1.4 Excluded from our work was:

- Any other payments by any other means e.g. Imprest account payments or similar
- Payments that were not readily identifiable via the bank statement e.g. no payee name/unclear payee name

2 AUDIT OBJECTIVES

2.1 The objective of our review is to provide assurance to management that for the period examined there are procedures in place both to prevent duplicate payments where at all possible, but also to detect and take corrective action if any have been made.

3 KEY FINDINGS AND RECOMMENDATIONS

Preventative Controls:

There are controls in the Payables module of the Agresso Business Management System to prevent duplicate payments. These are defined as follows:

- The Payables module of Agresso does not allow the same invoice number to be paid against the same supplier ID – this applied both to Purchase Order invoices & Supplier Order invoices.

However, duplicate payments could be made:

- If payments are made by via both Agresso payables module and an alternative method e.g. direct debit through the General business account.

- If a valid invoice is paid to both the valid supplier and accidentally to another

Work undertaken

3.1 We obtained a report of payments processed via Agresso for the financial year 2012/13. Although this identified 20,872 lines this included several lines against individual invoices where expenditure related to different cost centres. We used a data matching tool, IDEA to:-

Match on vendor name, invoice number & amount

- Match on vendor name, invoice number & amount for which there were over 1,800 matches. These were then matched with all the credit amounts to identify any credits that would offset the first payment and therefore a second payment was of no concern. As this only resulted in 2 matches the V000 9999 (VAT entries) were removed which left 1,000 lines of data.

- As it is unlikely that duplicate payments would be made on the same day, these 1,000 lines were sorted by 'transaction date' to identify any lines with duplicate information other than the transaction date. Only 1 record was shown as having a different transaction date to other records with the same vendor name and amount. However, this record had a different invoice number and order number and therefore not a duplicate payment

Match on invoice number and amount but not the supplier

- Match on invoice number and amount but not the supplier for which there were 8 matches. These payments were due to manual errors and had been made to the wrong supplier. Reimbursements have been received by either return of the payment or credit note received and payments made to the correct suppliers, therefore remedial action had been taken in respect of these duplicates.

Direct Debit Payments:

3.2 There is no list maintained of suppliers paid by direct debit but we were able to obtain details of 7 regular suppliers paid by this method and verified that no payments had been made to these suppliers via Agresso. The system enables a message to be entered on screen to alert staff if payment has been made by direct debit but this relies on communication between staff. Although there should be an option to select "direct debit" when setting up the method of payment for a supplier, this is not available as the option has not been configured.

Recommendation 1

Whilst no duplicate payments were found through being paid both by direct debit and through Agresso, consideration should be given to whether to record direct debit payments on Agresso to reduce the risk of a further payment being made through the application. This would be of increased importance if the volume of direct debit payments was to increase – *see also recommendation 3 for an alternative more robust way of recording payments to prevent duplicates.*

Electronic Payments via Bankline

3.3 A similar exercise was undertaken with the electronic payments made via bankline for the period April 2012 to March 2013. Where the payee was evident on the bank statements, these were compared to the suppliers payment file on Agresso, there were no matches. This process was manually undertaken because it was stated that an extract of payments could not be obtained from bankline, however it has now been ascertained that this is technically feasible and would therefore enable automated checking against the two systems in the future.

Recommendation 2

Consideration should be given to the ability to electronically extract and report transactions made through the bankline system, both for management reporting purposes and for any duplicate payment testing

3.4 Electronic payments through bankline are not recorded on Agresso.

Recommendation 3

Consideration should be given to recording in Agresso any payments made through alternative means other than the application e.g. direct debit, bankline etc. The standard way of achieving this would be to put the invoice and an identical credit note through Agresso (with same payment terms) & with a reference note useful both to the supplier and to the organisation e.g. 'contra entry – paid electronically'. This would ensure that the invoice was recorded within the system and so application controls to prevent a duplicate *(not allowing the same invoice number to be paid against the same supplier ID)* would be automatically employed should the invoice also be accidentally passed for payment via Agresso.

CONCLUSION

5 OPINION

Based on the answers provided during the audit and the testing undertaken, **substantial assurance** can be given that the internal controls in place to reduce exposure to those agreed risks currently material to the system's objectives are adequate and being managed effectively.

Although a number of important recommendations to bring about improvements have been made, none of these have a "high importance" rating signifying a particularly serious control weakness has been identified.

Management Agreed Action Plan

Rating

The **M** (amber background) symbol is denoted against recommendations where we consider the residual risk is significant enough to require action from management.

Ref	Expected Control or Testing Undertaken	Findings and Related Risks	Recommendation	Rating	Management Response	Responsible Officer Target Date
Control Objective 1: Effective controls are operating to prevent duplicate payments						
6.1	Controls should be employed to prevent payments by direct debit also being accidentally paid through the payables application	No such controls are employed *Increased risk of duplicate payments, albeit the current volume of direct debit payments reduces this risk.*	**Recommendation 1** Whilst no duplicate payments were found through being paid both by direct debit and through Agresso, consideration should be given to whether to record direct debit payments on Agresso to reduce the risk of a further payment being made through the application. This would be of increased importance if the volume of direct debit payments was to increase – see also recommendation 3 for an alternative more robust way of recording payments to prevent duplicates.		Agree- This also assists in meeting the new Transparency Code agenda. The issue has been raised at the Agresso Steering Group and a practical Technical Solution is being sought	Head of Finance June 2014

Ref	Expected Control or Testing Undertaken	Findings and Related Risks	Recommendation	Rating	Management Response	Responsible Officer Target Date
Control Objective 1: Effective controls are operating to prevent duplicate payments						
6.2	A list of payments through bankline (Nat West electronic banking system) can be extracted manually	LFRS were not able to produce any such listing, but it is our understanding that this is available from the system. *Increased risk of duplicate payments through the inability to electronically match against payments through Agresso*.	**Recommendation 2** Consideration should be given to the ability to electronically extract and report transactions made through the bankline system, both for management reporting purposes and for any duplicate payment testing		Agree – similar response to Recommendation 1.	Head of Finance June 2014

Ref	Expected Control or Testing Undertaken	Findings and Related Risks	Recommendation	Rating	Management Response	Responsible Officer Target Date
Control Objective 1: Effective controls are operating to prevent duplicate payments						
6.3	Controls should be employed in the main payables system (Agresso) to prevent payments that have been made through other methods being also paid through Agresso.	Payments made through bankline are not recorded through agresso. *Increased risk of duplicate payments,*	**Recommendation 3** Consideration should be given to recording in Agresso any payments made through alternative means other than the application e.g. direct debit, bankline etc. The standard way of achieving this would be to put the invoice and an identical credit note through Agresso (with same payment terms) & with a reference note useful both to the supplier and to the organisation e.g. 'contra entry – paid electronically'. This would ensure that the invoice was recorded within the system and so application controls to prevent a duplicate (not allowing the same invoice number to be paid against the same supplier ID) would be automatically employed should the invoice also be accidentally passed for payment via Agresso.		As noted in Recommendation 1, a practical technical solution is bing sought through the Regional Steering Group / Unit 4 direct.. Impementation timeframe to match the Transparency Code requirements.	Head of Finance June 2014

Appendix 4

Internal Audit Report

Leicestershire County Council
Leicestershire Fire & Rescue Service
Budget Monitoring
May 2014

KEY PERSONNEL	
Helen Moran	Senior Auditor
Matt Davis	Audit Manager
Neil Jones	Head of Internal Audit Service

INTERNAL AUDIT REPORT

LEICESTERSHIRE FIRE & RESCUE SERVICE

BUDGET MONITORING

MAY 2014

1 INTRODUCTION

1.1 A review of the revenue budget monitoring process was undertaken as part of the 2013/14 LFRS Internal Audit Plan.

1.2 The terms of engagement for the audit were agreed with Trevor Peel, Director of Finance and Corporate Services in March 2014.

2 AUDIT OBJECTIVES

2.1 We consider the objective of this audit is to ensure that controls in place to monitor the budget are robust.

3 KEY FINDINGS AND RECOMMENDATIONS

3.1 This report has been prepared on an exception basis. Where items have not been reported on below, you can draw confidence that controls are operating satisfactorily.

3.2 For those areas audited where recommendations are being suggested to help improve controls, details are presented in the Management Action Plan. For these particular areas we have listed the controls we would expect to find in place, what was actually in place, the resulting risks and our suggested recommendation to improve controls.

4 CONCLUSION

Budgets have been delegated where expenditure and income can be controlled locally. The view of budget holders as to the volume of training received varied, although there was a general view that more training would be beneficial.

Management information available to budget holders provided them with sufficient information to monitor budgets, although communication concerning when budgets have been loaded and any updates during the year could be improved.

Summary reporting is timely, accurate and provides adequate detail for decision-making. The budget position and any related issues are considered regularly at SMT and by members. Forecasts are produced by Finance and these were found to be based on valid assumptions.

The area of forecasting is one which we understand is to be further developed using existing AGRESSO capacity to record forecasts. This is likely to also include budget holders further in the process and therefore no specific recommendations have been made.

5 OPINION

Based on the answers provided during the audit and the testing undertaken, **substantial assurance** can be given that the internal controls in place to reduce exposure to those risks currently material to the system's objectives are adequate and are being managed effectively.

Although a number of important recommendations to bring about improvements have been made, none of these have "high importance" rating signifying a particularly serious control weakness has been identified.

Management Agreed Action Plan

Rating

The **M** (amber background) symbol is denoted against recommendations where we consider the residual risk is significant enough to require action from management.

Ref	Area	Findings	Recommendations	Rating	Management Response	Responsible Officer Target Date
Training and Support to Budget Holders						
1	ICQ to Budget Holders	The results of the questionnaire (ICQ) to budget holders have been provided to the Head of Finance for his consideration. The key areas which have been identified from the questionnaire are: • more information was required by budget holders as to when budget reports are ready to view at the start of the year and understanding how and when inflation , service changes and carry forwards are included in budgets. • Further training would be considered beneficial in the use of the Agresso reports, and instructions had not always been received on dealing with variances.	1. Consideration should be given to the following areas: - Regular email communications direct with budget holders to provide information on budgets being loaded, when updates occur (e.g. approval of carry forwards) and other general matters to assist in their understanding of their budgets and what is available from Agresso. - Training should be reviewed in terms of content and delivery, to address the issues identified by the audit questionnaire. These include: what information can be provided by Agresso and how to access it, minimum frequency for viewing reports,	**M**	Agree - this will be implemented Delivery / presentation on finance and budget issues will include the identified elements	Head of Finance June 2014

Ref	Area	Findings	Recommendations	Rating	Management Response	Responsible Officer Target Date
		However, although training in the use of the budget reports highlighted some concerns, the reports were generally considered to provide all the information required. In summary, further training was indicated as being of benefit by 3 of the 4 respondents. It should be noted however that the 4th respondent was from an area of the service that Finance had worked with more closely, and the responses here were very positive. Discussion with the Head of Finance indicated that it was his intention to deliver further training in a manner focussed to the recipients, rather than having one "general" session.	and how to deal with potential variances.			
2	Finance roles and responsibilities	Liaison with budget holders Returns from the sample of budget holders (Q3.5) indicated that scheduled meetings are not held with Finance to discuss budgets. Discussion with the Head of Finance indicated that there are regular meetings with budget holders in some areas, but	2.1 Regular meetings should be scheduled with all budget holders (at least twice yearly) to discuss their budget position and any actions required on variances. This would also provide an opportunity to identify training needs. Note: Frequency of meetings	**M**	Agree, however resource limitations have been a factor. I will work with the team to see how this can be best achieved.	Head of Finance June 2014

Ref	Area	Findings	Recommendations	Rating	Management Response	Responsible Officer Target Date
		that this does not happen across the service. Records of Training Provided Records are not currently retained when training is provided to budget holders, either in respect of the use of Agresso or other areas (e.g. when/how to escalate a variance). By maintaining records, accountability would be improved for both Finance and Budget Holders.	should be related to the inherent risk levels of each budget area. 2.2 Finance should maintain (brief) records of all future training provided to budget holders.	**M**	Agree that these will be maintained.	

Appendix 5

Internal Audit Report

Leicestershire Fire & Rescue Service (LFRS)
PWC Joint Audit - Key ICT Controls
March 2014

KEY PERSONNEL	
Jyoti Radia	**Senior ICT Auditor**
Matt Davis	**Audit Manager**
Neil Jones	**Head of Internal Audit Service**

INTERNAL AUDIT REPORT

LEICESTERSHIRE FIRE & RESCUE SERVICE

PWC JOINT AUDIT – KEY ICT CONTROLS

MARCH 2014

1 INTRODUCTION

1.1 A review of the ICT Controls operated within Leicestershire Fire & Rescue Service was undertaken as part of the 2013/14 audit plan covering key controls for the period 1 April 13 to 31 March 14. This work is carried out in accordance with PWC guidance as part of the joint audit.

2 AUDIT OBJECTIVES

2.1 We consider the overall control objective to be to ensure that the key ICT controls included in this review (per appendix 1) are operating effectively and efficiently.

Where in scope systems are referred to, these include:-

- Network
- Agresso (Financial)

Payroll functions are undertaken by Leicestershire County Council on behalf of LFRS and so Oracle Access is not afforded to LFRS staff.

3 KEY FINDINGS AND RECOMMENDATIONS

3.1 This report has been prepared on an exception basis. Where items have not been reported on below, you can draw confidence that controls are operating satisfactorily. The full list of controls reviewed is shown at Appendix 1.

3.2 For those areas audited where recommendations are being suggested to help improve controls, details are presented in the Management Action Plan. For these particular areas we have listed the controls we would expect to find in place, what was actually in place, the resulting risks and our suggested recommendation to improve controls within the system.

4 CONCLUSION

4.1 IT Organisation & Governance

There is an ICT structure in place with respective job descriptions that define key roles, responsibilities and reporting lines within ICT. There is an IT strategy in place to ensure that the priorities of the organisation are being met. Through the appropriate Steering Groups it is ensured that the ICT team provide systems that are aligned to the strategic priorities. There are two suggested areas for further development and these are the need for a review and update of the Internal ICT SLA document and the need to regularly report a dashboard of ICT performance statistics to Senior Management. Recommendation 1and Recommendation 2 apply.

4.2 IT Risk Management

There is a Corporate Risk Management framework in place and ICT risks are being documented. A Business Impact Analysis for ICT has been undertaken following the relocation to the new Birstall Headquarters. No recommendations have been made in this area.

4.3 IT Security

An annual independent penetration test has been undertaken. However transparency and documenting of actions being taken to address any vulnerabilities could be improved. This includes preparing an action plan promptly once the results of the test are received and the reporting of the results and progress against the actions to Senior Management. Recommendation 3 and Recommendation 4 apply.

4.4 Batch Processing

This area was agreed with PWC as out of scope for the 2013/14 review.

4.5 Network Security

Adequate system security in terms of capacity monitoring, backups, environmental controls in the server room and incident management is in place. However there is no formal DR Policy in place and a full DR test has not been undertaken since the move of the LFRS headquarters to Birstall. Recommendation 6 and Recommendation 7 applies.

In addition to this it was noted that although LFRS have a backup site, key servers are not mirrored. The mirroring of key servers would

improve resiliency in the event of an incident. Recommendation 5 applies.

4.6. **Systems Administration**

Testing on Agresso logical access controls, set up of starters on the system and removal of leavers from the system was concluded as satisfactory.

Testing on the network has identified an excessive number of grace logins allowed to a user if a password is entered incorrectly on the network. A recommendation has been made to reduce the number of grace logins. Recommendation 8 applies.

In addition to this, a user identified as having left the organisation in April 2013 still had access to the network at the time of the audit. This access has since been deleted. Recommendation 9 applies.

Furthermore, a list of inactive user accounts (e.g. those over 90 days) was obtained. It was noted that these accounts need further investigation as the last log on for some of these accounts date back to 2011 and 2012. Access to these accounts should be deleted if they are no longer required. Recommendation 10 applies.

4.7 **Privilege Users**

A formal privileged access policy should be considered and if adopted this should include user sign up and relevant management approval. See Recommendation 11. In addition to this, it was noted that there appears to be an excessive number of generic accounts set up. These need to be investigated and access removed where deemed appropriate. Recommendation 12 applies.

4.8 **Database Administration**

This area was agreed with PWC as out of scope for the 2013/14 review.

4.9 **New Applications and Systems**

The move to the new LFRS headquarters has required new IP addresses to be created, a second WAN and upgrades to the IP VPN connections from Virgin. At the time of the audit it was not possible to verify the success of the testing in these areas prior to implementation in a live environment due to a lack of documentation. See Recommendation 13

No other key systems have been implemented in 2013/14.

4.10 **Migration Errors**

This area was agreed with PWC as out of scope for the 2013/14 review.

4.11 **Regulatory Changes**

This area was agreed with PWC as out of scope for the 2013/14 review

4.12 **Change Control**

A draft Change Control Policy and Process document is in place. This has yet to be consulted with key stakeholders and approved by SMT. A high level review of the Change Control Policy has highlighted the need for further detail in certain areas. Recommendation14 applies.

4.13 **Change to Application Code**

This area was agreed with PWC as out of scope for the 2013/14 review

4.14 **Infrastructure and Configuration Changes**

This was covered as part of section 9. See section 4.9 above for the conclusion.

5 OPINION

Based on the answers provided during the audit and the testing undertaken, **substantial assurance** can be given that the internal controls in place to reduce exposure to those agreed risks currently material to the system's objectives are adequate and being managed effectively.

Management Agreed Action Plan

Rating

The **HI** (red background) symbol is denoted against recommendations where we consider the residual risk to be unacceptably high and this should be addressed by management urgently.
The **M** (amber background) symbol is denoted against recommendations where we consider the residual risk is significant enough to require action from management.
The **E** (white background) symbol denotes where there are potential efficiency gains from the action proposed.

Ref	Expected Control or Testing Undertaken	Findings and Related Risks	Recommendation	Rating	Management Response	Responsible Officer Target Date
Control Objective: IT Organisation and Governance						
6.1	Performance of IT activities and service delivery is monitored and reported to Senior Management.	There is an internal ICT Service Level Agreement (SLA) in place at LFRS which identifies the services offered by LFRS ICT to the Districts/Stations. It was noted that this SLA was dated July 2012 and was due for a review in August 2013. However, at the time of the review in January 2014, it was noted that this SLA had not been reviewed and updated. *Risk: Business requirements may not be met.*	**Recommendation 1** **The LFRS Internal ICT SLA should be reviewed and updated where relevant.**	**M**	SLA's will be updated and signed off by signatories by end of May 2014 Action on Service Delivery Manager Reporting SLA performance will not be made to Senior management.	Head of Information & Communications Services June 2014
6.2	Performance of IT activities and service delivery is monitored and reported to Senior Management.	It was confirmed by the ICT Systems Manager that ICT performance statistics available on the SpiceWorks system are currently not being reported to Senior Management.	**Recommendation 2** **Consideration should be given to producing a dashboard of statistics on ICT Service Delivery to enable performance**	**M**	Action Head of ICS, to establish appetite at SMT (Senior Management Team) for ICT service delivery metrics Business Analyst to	Head of Information & Communications Services June 2014

Ref	Expected Control or Testing Undertaken	Findings and Related Risks	Recommendation	Rating	Management Response	Responsible Officer Target Date
		Risk: Inadequate performance remains undetected resulting in no remedial action and therefore increased risk of network unavailability and non-fulfilment/late fulfilment of business requirements	**to be monitored and reported against to an appropriate oversight function**		provide sample reporting by End of May 2014	
Control Objective: IT Security						
6.3	A vulnerability assessment has been performed within the last 12 months and the results were promptly acted upon and reported to Senior Management.	The annual LFRS ICT independent penetration test was undertaken in February 2014. At the close of the audit in March 2014, it was noted that an action plan had not yet been produced from the penetration test results. The action plan from the 2013 could also not be obtained as assurance that all vulnerabilities identified as part of the test in 2013 had been addressed. This report highlighted that some applications were out-dated & insecure and this could lead to security weaknesses Furthermore there is currently no mechanism in place to report the findings and the results of action taken to mitigate the risks to the management team This was also highlighted as part of the 2012/13 PWC Key ICT Controls Audit. *Risk: Disruption to services and infrastructure,*	**Recommendation 3** **An action plan should be produced promptly from the penetration test output report. This should include the responsible officer, the target completion date and the action taken. This will ensure transparency and reporting that risks are considered and appropriately managed.** **Recommendation 4** **SMT should consider if**	**M** **M**	Action Service Delivery Manager to draw up Action plan by end of June 2014 and schedule tasks to be completed by November 2014 Head of ICS to establish if SMT or Security forum most	Head of Information & Communications Services June 2014 Head of Information & Communications Services

Ref	Expected Control or Testing Undertaken	Findings and Related Risks	Recommendation	Rating	Management Response	Responsible Officer Target Date
		poor utilisation of resources	**they wish the penetration results and associated remedial action and residual risks to be conveyed to them in order to satisfy themselves that appropriate timely action has been taken.**		appropriate representative body to report to by End of May 2014.	June 2014
Control Objective: Network Security						
6.4	Disaster Recovery Procedures are in place, are up to date, have been tested and cover all key areas.	LFRS ICT have a daily backup of all systems. The ICT Systems Manager confirmed that there is an ICT recovery site; however there is no full mirroring of key servers at present. *Risk: The agreed business requirements for ICT for service resumption may not be met leading to a disruption to services and infrastructure and poor utilisation of resources.*	**Recommendation 5** **Consideration should be given to the benefit versus cost implications for the mirroring of key ICT servers. A decision should then be agreed with Senior Management on whether key servers should be mirrored at the recovery site to ensure system resiliency.**	**M**	Action ICT Business Analyst to investigate DR solutions for key servers to include SQL mirroring. Project to be completed by March 2015. A mixed strategy will be adopted, mirroring or log shipping as appropriate and on the advice of vendors.	Head of Information & Communications Services June 2014
6.5	Disaster Recovery Procedures are in place, are up to date, have been tested and	ICT have a Business Continuity Planning (BCP) Business Impact Analysis specifically for ICT. However there is a lack of clarity on how the ICT BCP aligns with ICT Disaster Recovery (DR) and	**Recommendation 6** **A formal DR Process and Plan should be for**	**M**	Action Head of ICS to lead BCP BIA and ICT DR review and align where appropriate	Head of Information & Communications Services

Ref	Expected Control or Testing Undertaken	Findings and Related Risks	Recommendation	Rating	Management Response	Responsible Officer Target Date
	cover all key areas.	Corporate BCP requirements. Furthermore there was no documented DR plan & process The last DR test was a simulated test that was undertaken in 2012. However the results from this DR test were not documented and a recommendation to this effect was made within the 2012/13 PWC Key ICT Controls audit. A full DR test has therefore not been undertaken since the move to the new Birstall Headquarters in April 2013. *Risk: The agreed business requirements for ICT for service resumption may not be met leading to a disruption to services and infrastructure and poor utilisation of resources.*	**documented and this should align with Corporate BCP requirements.** **Recommendation 7** **A DR test should be undertaken especially now that LFRS Headquarters has now relocated to Birstall.**	**M**	Work to start August 2014 completion of documentation planned by end of Sept 2014 DR test scheduled for October 2014	June 2014 Head of Information & Communications Services June 2014
Control Objective: Systems Administration						
6.6	Passwords to the network, applications and operating system are utilised in an effective manner.	As raised within last year's PWC Key ICT Controls audit, the invalid login attempts is still currently set at 10 when best practice usually suggests grace logins from 3 to 5. This additional security is even more relevant in LFRS whereby access to the Agresso Financial System is via single sign on through the network.	**Recommendation 8** **The grace login parameters should be reduced to a lower level in line with industry best practice**	**M**	Action Service Delivery Manager, reduce grace login attempts to 8. End of May 2014. ICT management will not implement 3-5 grace logins. 8 Login attempts is sufficient to	Head of Information & Communications Services June 2014

Ref	Expected Control or Testing Undertaken	Findings and Related Risks	Recommendation	Rating	Management Response	Responsible Officer Target Date
		Risk: An increased risk of unauthorised access			protect ICT assets and maintain usability for end users on shift patterns without generating out of hours helpdesk calls.	
6.7	Leavers are promptly deleted from the network and applications.	A 100% check was undertaken using the IDEA interrogation tool to ensure that leavers identified on the Payroll System (Oracle) from April 2013 – February 2014 had been removed from both the network and the Agresso System. Exceptions identified from the IDEA interrogation were investigated in detail and it was concluded that in one instance a leaver's access had not been removed from the network. This account was deleted at the time of the review and it was confirmed that the user had not logged onto the network after they had left. At the time of the audit, a report was obtained of accounts on the network that have been inactive for over 90 days. This report highlighted thirteen accounts that were last used in 2011/2012. Three of these were user accounts whilst ten of these were generic accounts. *Risk: An increased risk of unauthorised access and also an inability to detect if any unauthorised*	**Recommendation 9** **A revised system for deleting inactive accounts from the network should be considered to ensure that accounts no longer required are promptly deleted from the system.** **Recommendation 10** **A review should be undertaken on the report detailing the accounts that have not been used in the last 90 days to determine if they are still**	**M**	A revised process is now in place using SharePoint alerts on leavers list maintained by HR are set to IT helpdesk which auto-generates a ticket for action. Ticket details include last working date and expected last day at work, to cover people who take leave before final end date. Action Service Delivery Manager to feedback on accounts with specific purposes and those not used in 90 days by End of May 2014	Head of Information & Communications Services June 2014 Head of Information & Communications Services June 2014

Ref	Expected Control or Testing Undertaken	Findings and Related Risks	Recommendation	Rating	Management Response	Responsible Officer Target Date
		business use had occurred after date of leaving.	**required. (Especially the accounts that were last logged into in 2011 and 2012).**			
Control Objective: Privilege Users						
6.8	There is a Privileged Access Policy in place and privileged access user accounts are monitored.	At present there is no Privilege User Policy in place to govern high level access rights that are afforded to some users. These access rights are deemed higher risk as it enables these users to undertake administrative tasks, that if misused could cause major disruption to ICT Services. The lack of a formal Privilege Access Policy was also raised as part of the 2012/13 PWC Key ICT Controls Audit and a recommendation made to this effect. LFRS consider that the monitoring of the privilege user accounts is not practical therefore this risk is tolerated by LFRS Senior Management. *Risk: Access rights afforded are not commensurate with business requirements, use of such access rights is not defined and they are not authorised leading to an increased risk of unauthorised processing and compromise of the IT infrastructure and associated applications.*	**Recommendation 11** **Consideration should be given to adopting a privileged access policy and process through which responsibilities for privileged users are documented and signed against and relevant management then formally approve such access for a time limited period**	**M**	Action ICT Systems Manager review statement for external users and modify for ICT personnel to sign up to. A policy will be created to cover privilege users end of July 2014 Management comment: The agreement will not be time limited, it is expected the statement will apply for the duration of the employment of the signatory	Head of Information & Communications Services June 2014

Ref	Expected Control or Testing Undertaken	Findings and Related Risks	Recommendation	Rating	Management Response	Responsible Officer Target Date
6.9	Where possible accounts have been assigned to individual users.	A list of generic accounts currently set up on the Network and Agresso were examined. Testing confirmed that there are 186 generic network accounts that have been set up. Further investigation is therefore required on whether these generic accounts are still valid or whether they can be deleted. *Risk: Misuse of the network through the use of a generic account no longer in use. Actions cannot be traced to an individual.*	**Recommendation 12** **A review should be undertaken of generic accounts that have been set up for the network and access should be removed where there is no longer a business need for this account. If from this review it indicates that the accounts are no longer needed then revised procedures should be considered for the control of generic accounts**	**M**	Action Service Delivery Manager review of 'Generic' accounts to be completed by end of May 2014. Many of the accounts classed as 'generic' have specific purposes. Action ICT Systems Manager Catalogue of generic account ownership, reason for account, who has access or knowledge of account login (if there is one) and any deletion date to be created by end of July 2014	Head of Information & Communications Services June 2014
Control Objective: New Applications and Systems						
6.10	New systems and enhancements are adequately tested/ authorised.	In 2013/14 LFRS moved from the Glenfield Headquarters to Birstall. This moved required various changes to the ICT infrastructure. The key changes were:- • Move of the entire server farm to Birstall (change of IP addresses) • Implementation of a second WAN (Wide Area Network)	**Recommendation 13** **Documentation supporting the testing of a major change to the ICT infrastructure should be retained as evidence that testing was concluded as**	**M**	Action Head of ICS to review proposed draft policy end of June 2014. Action Service Delivery Manager to create change form and process for testing and completion of ICT	Head of Information & Communications Services June 2014

Ref	Expected Control or Testing Undertaken	Findings and Related Risks	Recommendation	Rating	Management Response	Responsible Officer Target Date
		• Upgrade to the Shepshed and Stores IPVPN connections. The IT Systems Manager confirmed that all the above changes were tested where possible; however no supporting test documentation had been retained. *Risk: Failure of the LFRS network.*	**successful before being implemented in a live environment.**		infrastructure changes End of June 2014.	
Control Objective: Change Control						
6.11	Changes to the network and applications are subject to a formal change control process.	A recommendation was made as part of the 2012/13 audit on the need for a formal Change Control Policy and Process. It has been identified that a draft Change Control Policy has been developed. This Policy has yet to be agreed with key stakeholders and SMT. At present there is no consistent way in which changes to the IT infrastructure and applications are dealt. Once the Change Control Policy and Process has been approved this will ensure that all changes undergo a formal assessment and approval process. A high level review of the draft Change Control Policy has highlighted that the policy document and the change form need to be updated to include further detail on the documentation for assessing the risk of implementing/not implementing a change, back-out options available, prioritisation of change	**Recommendation 14** **The draft Change Control Policy and Process should be further developed to include more detail on assessing the risk of implementing/not implementing a change, back-out options available, prioritisation of change requests etc and then signed off for use within the organisation.** ***Further Internal Audit***	**M**	Action Head of ICS to create overall Change Control policy and process End of August 2014.	Head of Information & Communications Services June 2014

Ref	Expected Control or Testing Undertaken	Findings and Related Risks	Recommendation	Rating	Management Response	Responsible Officer Target Date
		requests etc. *Risk: Disruption to services and infrastructure, poor utilisation of resources*	***advice may be available if required in respect of the suggested updates.***			

APPENDIX 1

System Control Objectives

- **1. IT Organisation & Governance**
  - How is the IT function structured and has this been documented?

- **2. IT Risk Management**
  - What is management's process for identifying and managing risk within the IT environment? Who leads this and how is it reported upon? Is this integrated with the corporate risk management process?

- **3. IT Security**
  - What IT Security Policies relating to Information Security, Internet and Acceptable Use of IT/email are in place?
  - How are IT assets (software and hardware) recorded and tracked?
  - What physical security controls are in place to protect key IT assets, such as the main system servers and communications room? Visit the data centre and observe entry requirements e.g. restricted to authorised personnel through key code locks, swipe card access, visitor logs, locked server cabinets etc.
  - Is anti-virus / anti-malware software in place to reduce the risk that malicious software could be introduced and affect systems? How often is this updated? Is this automatically deployed and is this monitored?
  - What ensures that external access is subject to an appropriate level of control with specific controls over external network access (dial-in, network to network access, such as firewalls, VPN tokens etc), and controls are in place to monitor network security (including firewall log monitoring, and intrusion detection systems)?
  - Are the external network connection points documented? Has a vulnerability assessment been performed within the last 12 months (e.g. attack and penetration test; external/internal or both)? If so, what were the results, and were they acted upon?
  - Are changes to network devises and configuration (e.g. firewalls, routers, DMZ) subject to formal change control procedures?

- **4. Batch Processing**
  - Only approved and tested changes are made to the batch scheduler
  - Errors in production processing are identified and resolved.

- **5. Network Security**
  - Errors in production processing are identified and resolved.
  - Data is appropriately backed up and recoverable.

- **6. Systems Administration**
  - Passwords to applications are utilized in an effective manner
  - Passwords to the operating system/network are utilized in an effective manner.
  - Access requests to the application are properly reviewed and authorized by management, both for internal users and 3rd parties.
  - Access requests to the operating system/ network are properly reviewed and authorized by management, both for internal users and 3rd parties.
  - Terminated application user access rights are removed on a timely basis.
  - Terminated operating system/ network user access rights are removed on a timely basis.
  - Access rights to applications are periodically monitored for appropriateness, including audit logging and security configurations over the applications.
  - Access rights to the operating system/ network are periodically monitored for appropriateness, including audit logging and security configurations over the applications.

- **7. Privilege Users**
  - Policies are maintained for segregation of duties within IT.
  - Super-user/administration application transactions and activities are monitored.
  - Super-user/administrative database/data file transactions and activities are monitored.
  - Super-user/administrative operating system/network transactions and activities are monitored.

- **8. Database Administration**
  - Access requests to the database/date file are properly reviewed and authorized by management, both for internal users and 3rd parties.
  - Terminated database/data file user access rights are removed on a timely basis.
  - Super user/administrative database/data file transactions and activities are monitored.
  - Access rights to the database/data file are periodically monitored for appropriateness, including audit logging and security configuration of the database and key financial data.
  - Passwords to the database/data file are utilized in an effective manner.

- **9. New Applications and Systems**
  - New systems/major enhancements are adequately tested or authorized.
  - Only properly approved new system/major enhancements are migrated into production.
  - Problems during program development are monitored and resolved.
  - Errors in production processing are identified and resolved.

- **10. Migration Errors**
  - Data is properly migrated/converted.

- **11. Regulatory Changes**
  - Changes requested and processed to application programs are recorded and periodically monitored for appropriateness.
  - Changes requested and processed to application configurations are recorded and periodically monitored for appropriateness.

- **12 Change Control**
  - Changes requested and processed to application programs are recorded and periodically monitored for appropriateness.
  - Changes requested and processed to application configurations are recorded and periodically monitored for appropriateness.
  - Changes to application programs are adequately tested.
  - Only properly approved changes to application programs are migrated into production.
  - Only properly approved changes to application configurations are migrated into production.
  - Development, testing and production environments are segregated for changes to application programs.
  - Developments testing and production environments are segregated for changes to application configuration.
  - Errors in production processing are identified and resolved.

- **13. Change to Application Code**
  - Policies are maintained for segregation of duties within IT.
  - Access requests to the operating system/network are properly reviewed and authorized by management.
  - Terminated operating system/network user access rights are removed on a timely basis.
  - Access rights to the operating system/network are periodically monitored for appropriateness.
  - Emergency changes to application programs are adequately tested and authorizes after implementation.
  - Emergency changes to application configurations are adequately tested and authorized after implementation.

- **14. Configuration & Infrastructure Changes**
  - Changes to the Operating System/Network/database are adequately tested.
  - Only property approved changes to operating system/network/Database are migrated into production.
  - Changes processed to the Operating System/network/Database is periodically monitored for appropriateness.
  - Emergency changes to the operating system/network/database are adequately tested and authorized after implementation.

Appendix 6

Internal Audit Report

Leicestershire County Council
Leicestershire Fire & Rescue Service
Payroll 2013-14 - Final Audit
July 2014

KEY PERSONNEL	
Lynn Woolhouse	Auditor
Matt Davis	Audit Manager
Neil Jones	Head of Internal Audit Service

FINAL INTERNAL AUDIT REPORT

LEICESTERSHIRE FIRE & RESCUE SERVICE

PAYROLL 2013-14 – FINAL AUDIT

JULY 2014

1 INTRODUCTION

1.1 A review of the procedures in place for administering starters, leavers and variations to pay including deductions, relating to Leicestershire Fire and Rescue Service (LFRS) employees and pensioners was undertaken as part of the 2013/14 LFRS Internal Audit Plan.

This audit will assist the external auditors, Price Waterhouse Coopers, in their annual assessment of the likelihood of material misstatement in the Combined Fire Authority's financial accounts.

1.2 At the start of 2013/14 financial year LFRS employed just over 859 operational and non-operational staff. The budgeted figure for payroll laid down in the Medium Term Financial Strategy for LFRS was just under £28.6 million. The Human Resources (HR) and Finance sections are responsible for making sure all data is current and up to date, this information is then forwarded to East Midlands Shared Services (EMSS) Payroll for inputting onto the payroll system and subsequent payment.

1.3 This is the second review covering periods nine to twelve (December to March), the initial review covered periods one to eight (April to November) and a report was issued in March. Sample sizes having been agreed with PWC.

2 AUDIT OBJECTIVES

2.1 The control objectives for this audit are to ensure that:-

- All new members of staff are bona-fide, are paid at the correct rate and from the correct date.
- All leavers are paid up to the correct date and all relevant expenses and advances are recovered.
- All variations to pay are valid with correct authorisation and for the correct amount.
- Deductions from pay are accurate and supporting documentation retained.

3 KEY FINDINGS AND RECOMMENDATIONS

3.1 This report has been prepared on an exception basis. Where items have not been reported on below, you can draw confidence that, from the sample examined, controls are operating satisfactorily. The full list of controls reviewed is shown at Appendix 1.

3.2 For those areas audited where recommendations are being suggested to help improve controls, details are presented in the Management Action Plan. For these particular areas we have listed the controls we would expect to find in place, what was actually in place, the resulting risks and our suggested recommendation to improve controls.

4 CONCLUSION

4.1 Documentary evidence exists to support the creation of sampled new starters and initial salary payments agreed to contractual information.

4.2 For the sample selected of staff that have left the employ of LFRS final payments were found to have been calculated to the correct leaving date and, in all but one case, where necessary, relevant expenses recovered or salary owing (e.g. TOIL, holiday pay) paid. The error detected is detailed within the next section. (see recommendation 1 & 2)

4.3 Variations to pay / deductions from pay were found to be accurate and supported by relevant documentation.

5 OPINION

Based on the testing undertaken during the audit, **substantial assurance** can be given that the internal controls tested are operating adequately as intended to reduce exposure to those associated risks currently material to the system's objectives.

Although a number of important recommendations to bring about improvements have been made, none of these have "high importance" rating signifying a particularly serious control weakness has been identified.

Management Agreed Action Plan

Rating

The **M** (amber background) symbol is denoted against recommendations where we consider the residual risk is significant enough to require action from management.

Ref	Testing Undertaken	Findings and Related Risks	Recommendation	Rating	Management Response	Responsible Officer Target Date
CONTROL OBJECTIVE: All leavers are paid up to the correct date and all relevant expenses and advances are recovered						
5.1	From the report provided by LFRS of service leavers between 1 April 2013 & 31 March 2014 sixteen records were selected to verify that payment was calculated to the correct leaving date and that relevant expenses recovered or salary owing (e.g. TOIL, holiday pay) paid.	For all records sampled payment was found to have been calculated to the correct leaving date. Where specific instruction was given to either pay holiday owing or recover overpayment of holiday this too was found to be correct with one exception. Post No. 0582 (AM) ceased employment of both contracts on 6 April 2013. Instruction was given to pay holiday owing of £214.78. EMSS erroneously applied this payment to both contracts.	1. LFRS should decide if any recovery is necessary. 2. Where the leaver holds a dual contract, and both positions are being terminated, consideration should be given to issuing separate notification of leaving forms to EMSS so that instruction may not be misconstrued.	**M** **M**	Advised by email (1-7-14) that EMSS has been instructed to pursue recovery of the overpayment. Agree the recommendation and this will be implemented for future occurrences.	n/a Finance Manager September 2014

APPENDIX 1

System Control Objectives

1. Starters:-
   - The organisation should comply with all Inland Revenue and DSS regulations.
   - There should be independent documentary evidence to support the creation of a new employee record.
   - All starters should be initiated and recorded promptly.
   - The person commencing employment should be bona fide.

2. Leavers:-
   - The organisation should comply with all Inland Revenue and DSS regulations.
   - All leavers should be authorised properly.
   - There should be documentary evidence to support an employee leaving a post.
   - All relevant parties should be informed of an employee leaving in order that records may be updated.
   - All relevant records should be updated correctly when an employee leaves.
   - All monies owing to the organisation should be calculated correctly and repaid promptly.
   - Employees leaving the organisation should not be paid beyond their leaving date.

3. Deductions:-
   - There should be documentary evidence to support all deduction transactions.

4. Variations:-
   - All amendments to payments, e.g. overtime, should be in accordance with standing orders and financial regulations.
   - All amendments to pay should be supported by written documentation.
   - All input in respect of standing and temporary data should be legitimate and appropriate.

Appendix 7

Internal Audit Report

Leicestershire Fire & Rescue Service

Risk Management

April 2014

KEY PERSONNEL	
Jay Manager	Senior Auditor
Neil Jones	Head of Internal Audit Service

INTERNAL AUDIT REPORT

LEICESTERSHIRE FIRE & RESCUE SERVICE

RISK MANAGEMENT

APRIL 2014

1 INTRODUCTION

1.1 A review of the risk management framework was undertaken as part of the 2013/14 Leicestershire Fire & Rescue Service (LFRS) Internal Audit Plan.

1.2 Further detail as to the background to the audit can be seen in the Terms of Engagement as shared for agreement with Director of Community Services, Director of Finance and Corporate Resources and Head of Finance. This shows the risks, scope and methodology adopted to undertake the audit. This document is available upon request.

2 AUDIT OBJECTIVES

2.1 The objective of our review is to provide assurance to management that the risk management framework* is effective in assisting the CFA achieve its objectives.
(Corporate Risk Register only)*

3 KEY FINDINGS AND RECOMMENDATIONS

3.1 This report has been prepared on an exception basis. Where items have not been reported on below, you can draw confidence that controls are operating satisfactorily.

3.2 For those areas audited where recommendations are being suggested to help improve controls, details are presented in the Management Action Plan.

4 CONCLUSION

There is evidence that some risk management activities are operating adequately. LFRS has in place a Corporate Risk Management (RM) Procedure and associated guidance (the Procedure). This was reviewed, updated and approved in July 2011 by the SMT. The responsibilities of the CFA, SMT and Risk Management Group (RMG) are stated in the Procedure. The Corporate Risk Register consists of risks derived from Our Plan - Action Plan tasks. Risk assessments (CRAFTS) are in place for all risks on the Corporate Risk Register. The RMG met regularly in the earlier part of 2013 to review and update the

Corporate Risk Register. New risks are identified for inclusion, for example industrial action has been added recently.

However, based on our knowledge of best practices noted we consider there are a number of areas where the framework could be improved and strengthened, some of which the Service itself has already acknowledged:

- The Corporate Risk Register (CRR) largely consists of project risks identified from the Action Plan tasks which stem from Our Plan. However, key projects are already monitored monthly by the SMT, Policy and Overview and Scrutiny Committee. It is acknowledged that although some key projects warrant inclusion on the CRR due to the nature and significance of risks identified, there is some duplication. Conversely, other significant risks stemming from Health & Safety (e.g. serious death or injury) or the Integrated Risk Management Plan (National Framework) are not included on the CRR. This has already been acknowledged by the Service and is a main driver for review of the existing procedures.

- Individual directorate plans were not provided and therefore it was not possible to ascertain the flow of any key risks from these into the CRR, however, risks such as MTFS savings are identified.

- LFRS's Our Plan is supported by an Action Plan but this provides details of key projects only. It is unclear whether of all key risks that affect the achievement of the strategic objectives stemming from Our Plan are captured in the register.

- There are no clearly defined processes in place for setting, approving, monitoring, and communicating risk tolerance levels for all major types of risks. Therefore all risks appear on the CRR even those classed as low or medium. To ensure the CRR is focused and identifies key strategic risks, defined thresholds with clear escalation procedures need to be established. This has been acknowledged by the Service and will be addressed within the new Procedure.

- The Annual Governance Statement for 2012-13 states that the Risk Management Group, reports progress on mitigating the risks in the CRR to the Policy Committee. However, the audit did not identify any specific reports. This has been acknowledged by the Service and the future roles and responsibilities including reporting lines are going to be clarified and clearly defined within the Procedure.

- Regular reporting of the CRR to SMT has not been in place for the latter part of the year as the role of the Corporate Risk Management Group was re-defined and the group integrated

within the Health & Safety Group (HSW&CRMG). Regular reporting of the CRR is undertaken to the HSW&CRMG (formally the RMG) which is made up of members of the SMT. There was no formal reporting to SMT as it would represent duplication of effort.

- All risks on the CRR are supported by risk assessment templates (CRAFTS) but these are not regularly reviewed or updated. The on-going monitoring and update to changes in risks (if any) is reflected on the CRR itself. Therefore it is not possible to ascertain whether any further key actions agreed on the templates are completed by the timescales assigned.

Future Direction

In February 2012 LFRS participated in a Peer Challenge, and this identified that there was room to consider improvements to the integration of risk management processes within the Service. The Annual Governance Statement for 2012/13 also identified this area as a minor governance issue.

As a result, work has been undertaken during 2013 to assess and review the current procedures and the Director of Community Services plans that this will be finalised in June 2014 for consideration and approval by SMT.

The Director of Community Services acknowledges that risk management activities are not coordinated across the differing service areas to ensure that no major risk is overlooked. At the time of the audit the Service had already acknowledged that there are there are differing policies and related risk assessment processes for Health & Safety, Project Risks etc. but these are not interlinked to demonstrate a clear integrated risk management approach. The Director envisages that a single comprehensive Procedure would reduce potential duplication, provide greater clarity, consistency and result in a comprehensive Corporate Risk Register

5 OPINION

At the time of testing, we found that transitional arrangements were in place but there was an acknowledgement that there was scope for improvements including:

* An integrated risk management process and single framework for all areas of the service
* Comprehensive Corporate Risk Register to fully capture all key risks

As such **reasonable assurance** can be given that the internal controls in place to reduce exposure to those risks currently material to the system's objectives are adequate and are being managed.

On this occasion, before concluding the final report, we have been advised by the Director of Community Services that action is being taken to implement a new Risk Management Procedure. We will test implementation during 2014-15 to ensure controls are operating satisfactorily, and as such the direction of travel would be towards **substantial assurance.**

MANAGEMENT AGREED ACTION PLAN

Rating
The **M** (amber background) symbol is denoted against recommendations where we consider the residual risk is significant enough to require action from management.

Ref	Recommendation	Rating	Management Response	Responsible Officer Target Date
6.1	An effective integrated framework for risk management should be developed and implemented The following are some of the fundamental areas that could be considered within any revised framework being proposed : Procedure and Guidance • Risk Management (RM) Procedure should ensure alignment to Corporate documents for example Our Plan, Directorate Plans, Project Risks and other policies (Health & Safety) • The roles and responsibilities including any reporting should be outlined • Terms of Reference for the Risk Management Group including others should be developed ensuring appropriate membership • The risk appetite should be agreed and specified within the Procedure • Risk tolerance levels and escalation procedures should be established, approved and reviewed and adjusted annually if appropriate • Approval of the Procedure including on-going review Corporate Risk Register (CRR) • Comprehensive review of the CRR which encompasses all risks for example, Strategic, Tactical, Corporate and Operational • The CRR should be refreshed with a view to reducing the number of risks to a manageable level and reflecting more accurately the current position. This will ensure that major risks are escalated to SMT (and appropriate Committee) for consideration. • Timely reporting of the CRR to the relevant oversight bodies • Development of Directorate risk registers at all service specific levels	**M**	Agreed	Director of Community Services August 2014

Ref	Recommendation	Rating	Management Response	Responsible Officer Target Date
	• The need to ensure the CRR and associated documentation – templates) are fully completed, monitored regularly, and kept up to date. For example: o Appropriate ownership of risk and then assignment to control owners including access to CRAFTs via SharePoint to facilitate easier updates o Regular review and update by risk owners prior to meeting o Assignment of realistic timescales to further actions and then subsequent review to ensure completed and the residual adjusted if appropriate o Removal of risk no longer relevant Training • Scope for communication of the Procedure and development of a training infrastructure to support all stakeholders in meeting their specified roles and responsibilities for risk management • Member training if appropriate			

Appendi

Internal Audit Report

Leicestershire Fire & Rescue Service
Duplicate Training Claims
March 2013

KEY PERSONNEL	
Dianne Harris	Auditor
Matt Davis	Audit Manager
Neil Jones	Head of Internal Audit Service

DRAFT INTERNAL AUDIT REPORT

LEICESTERSHIRE FIRE & RESCUE SERVICE (LFRS)

DUPLICATE TRAINING CLAIMS

MARCH 2013

1 BACKGROUND

1.1 Following an incident which ultimately led to disciplinary action, a request was received from the Director of Finance & Corporate Services, Trevor Peel, requesting that an audit was undertaken to examine the revised processes in place to enable Retained Fire Fighters to claim reimbursement for loss of earnings (from any employment) following attendance at training courses.

1.2 A situation had arisen whereby a Retained Fire Fighter had submitted three duplicate claims for reimbursement of loss of earnings for attendance at training courses, the total value of claims being £1,094.40 (gross). The duplicate claims were identified by the LF&RS Firewatch Co-ordinator following a request to provide information on expenses claimed.

1.3 In order to claim for loss of earnings a training claim form is required to be completed. Once certified this claim is then processed through the LCC Oracle HR system. It was found that, in addition to claiming for loss of earnings on the training claim form, the employee had also claimed attendance at a 'drill' on the same day on a certified Firewatch electronic timesheet recording system, which then resulted in payments being made from both the Firewatch system and via the training claim form. The Firewatch system is not ordinarily used to claim for time spent attending training courses and the duplication had only occurred due to the time being erroneously, and through disciplinary hearing was deemed to be deliberately claimed as "drill" time.

1.4 Time recorded on the Firewatch system is required to be authorised by line management.

1.5 Disciplinary action has been taken against the employee concerned, and it is our understanding that repayment of the overpayment has been made.

2 SCOPE

2.1 The scope of the audit (as agreed with the Director of Finance & Corporate Service) includes a review of: -

- How the duplicate claims were identified
- Whether weaknesses are apparent in the use of either the Firewatch and/or the Oracle HR system for claiming training expenses
- Examination of preventative and detective controls and an assessment of whether (and, if so, where) key internal controls failed
- Safeguards in place to prevent similar occurrences and methods used to communicate this within the organisation
- Whether revised procedures would be likely to prevent this happening again
- What steps have been taken to investigate the possibility of other such occurrences and provide an opinion on the adequacy of these
- Ascertain if there are any weaknesses / system vulnerabilities in Oracle HR in relation to the processing of training claims

2.2 This audit has not examined, and will not be providing an opinion on, the disciplinary action taken by LFRS on this matter. It is our understanding that disciplinary action has now concluded in respect of the individual concerned and that the matter is considered to be closed, unless any further instances come to light in which case it is understood that any action taken will be consistent with that already applied.

2.3 During the course of this audit discussions have taken place with:

- Finance Office Manager
- Assistant Finance Office Manager
- The Head of HR
- Firewatch Co-ordinator
- Training Administrator

3 KEY FINDINGS

3.1 How the duplicate claims were identified

The duplicate claims were identified following a request from the authorising manager to the Firewatch Co-ordinator regarding the particular expense claims. Reports from Firewatch were compared to training claims held by the Finance Section and it was identified that the employee had submitted training claims for the same dates as attendance at drills had been recorded on Firewatch.

3.2 Weaknesses apparent in the use of Firewatch and Oracle for claiming training expenses

LFRS has confirmed that all employees that use the Firewatch system to record their time are aware that where they attend training they should complete a training claim form in order to be reimbursed for loss of earnings and should not record any time relating to training on the Firewatch system. Indeed, it is understood that there is no such "training" option / category available on Firewatch.

The reports produced by the Firewatch Co-ordinator had identified instances where an employee had recorded hours on Firewatch for a 'drill' on the same day where a training claim form had been completed for reimbursement of loss of earnings whilst attending training. The hours recorded on the Firewatch system are ordinarily authorised by line management. In the circumstances of this case, it may not have been easy to confirm that the attendance recorded on the timesheet was correct. This weakness in internal control (independent authorisation) is likely to have contributed towards the irregularity.

Based on the work undertaken there is little scope for *inadvertent* duplication of claims as the Firewatch system does not have a "training" option / category. In this instance, the duplication has occurred as a result of an individual submitting a training claim for loss of earnings as well as claiming for attendance at a drill session on Firewatch at the same time. It is difficult to see that this could be anything other than a purposeful attempt to double-claim for time. This was similarly concluded at the internal disciplinary investigation. (Recommendation 1)

3.3 **Examination of preventative and detective controls**

Both the Finance Office Manager and Assistant Finance Office Manager have confirmed that, at the time the duplicate claims were identified, although verbal instructions had been given to employees how to claim for loss of earnings whilst attending training there were no clear documented written procedures. This left the Service vulnerable as good practice suggests that employees should be provided with clear guidance to follow as, if there is no guidance, employees could make genuine mistakes when making claims for loss of earnings (Recommendation 2) – see also immediately below.

3.4 **Safeguards in place to prevent similar occurrences and methods used to communicate this**

It has been confirmed that procedures are currently being drawn up regarding how to claim for loss of earnings when attending training and these should be completed shortly. The Training Department issued guidance in December within a weekly bulletin regarding how claims for loss of earnings should be made and will be producing a PowerPoint presentation in to be used at training events (Recommendation 3).

The LF&RS Training Department is required to sign each completed training claim forms to confirm that the training was attended. The Training Administrator maintains a record of who has attended training and records when a claim form has been received. Once recorded the training claim forms are then sent to the Finance Section to be processed for payment. The Assistant Finance Office Manager has confirmed that if the training claim form has not been signed by the Training Administrator no payment will be made and the form is returned to the Training Unit to complete.

3.5 **Whether revised procedures would prevent this happening again**

Whilst revised procedures are likely to assist employees in knowing what is expected when claiming for loss of earnings, the Service need to be able to demonstrate that employees have received and understood the procedures as they could still face challenge if an employee was to say that he/she was not aware of the correct procedures to follow. (Recommendation 2)

3.6 **Ascertain what steps have been taken to investigate the possibility of other such occurrences and provide an opinion on this**

Following identification of the duplicate payments the Finance Office Manager and Assistant Finance Office Manager have compared training records to Firewatch claims going back three years. These members of staff have confirmed that this exercise identified three further instances where duplicate claims had been made by employees. Finance staff has investigated these other claims further and they were considered to be genuine mistakes and no further action was taken. It should be noted that no further testing has been conducted by Internal Audit in this area and an assumption made that if any further instances come to light then any action taken will be consistent with that already applied

3.7 **Ascertain if there are any known weaknesses / system vulnerabilities in Oracle HR.**

No weaknesses have been identified in processing through the Oracle HR application. Training claim forms have been processed correctly and accurately and, where duplications have occurred, this has been as a result of erroneous claims being processed via the Firewatch system (the output of which is transferred to Oracle HR via spreadsheet upload). Training claim form completion and subsequent processing via Oracle HR remains the system to be used to process loss of earnings as a result of attendance on training courses and LFRS has confidence that it does so effectively.

4 CONCLUSIONS

4.1 The Service has stated that this duplication, although considered by them to have been fraudulent rather than inadvertent, is not due to any particular software vulnerabilities in either the Firewatch or Oracle HR systems. The Firewatch system does not in itself provide for attendance at training courses to be claimed for, and the duplicate claims only occurred as a result of an incorrect disturbance category being recorded on Firewatch (recorded as attendance at a drill rather than as training).

There is always an inherent risk of an individual claiming time, for example at a drill, on occasions not actually worked. Ordinarily, the preventative control is that all time claimed via Firewatch has to be authorised prior to processing. This gives the authorising officer scope to confirm that time recorded was indeed worked prior to releasing claims for payment.

In this instance, It may not have been easy to confirm that the attendance recorded on the timesheet was correct and a result there is a heightened risk of financial irregularity. The Service has decided to accept this risk when considering the impact and likelihood of this occurring in comparison to the practicality and efficiency of operation.

The alternative longer term option could be for the Service to explore whether Firewatch can be modified to process claims for loss of earnings whilst attending training. This would eradicate the need for completion of training claim forms.

4.2 Following identification of the duplicate payments, the action taken by the Service has been found to be satisfactory in seeking to prevent such instances occurring in the future. For example, there has been a recent bulletin reinforcing the processes to be followed regarding claiming for attendance at training courses.

4.3 The Finance Section has confirmed that they have undertaken a thorough review of other claims for training over the past three years to gain assurances that there have not been other duplicate payments processed in a similar manner, whether inadvertent or fraudulent. Internal Audit has not sought to re-perform these "assurance" tests and therefore management is presently solely reliant on the confidence that the Finance Section has in that this issue was isolated. Although Finance Section checks did identify a small number of other overpayments, these have been investigated and concluded by the service to have been inadvertent errors rather than fraudulent in nature. It is understood that LFRS has taken steps to recover any amounts overpaid / over claimed and management are confident that the lesser action taken against these individuals compared to the main perpetrator can be justified

4.4 The service should consider preventative controls (see Recommendation 1). It is recognised; however, that there will be a cost associated with these additional, albeit sample, checks, and the service needs to consider whether the cost of the additional checks outweighs the risk of possible further duplicate claims.

4.6 It is important that the Service continues to regularly reiterate clear guidance to employees as to how to claim for loss of earnings, and that this is also made clear at training events.

5 RECOMMENDATIONS

Recommendation 1

As a preventative control, the Service should consider if they wish to introduce a system whereby, when employees have completed a training claim form, the dates of training are compared by the Finance Section to Firewatch electronic timesheets to ensure that any additional time claimed on that day relates purely to hours attended at work and not for training. These checks could be undertaken on a sample-check basis.

Recommendation 2

The Service should produce and circulate clear procedures which should be followed when making claims for loss of earnings. This should include circumstances where the loss of earnings is in relation to attendance at training courses. There may be a need to clarify and distinguish what constitutes “training” to be claimed via Oracle HR (e.g. attendance on a course) and what constitutes overtime claimable via Firewatch, even if “training” by nature (e.g. drill nights could conceivably be considered to be training). Once complete these should be issued to all relevant staff and if possible uploaded to the LFRS Intranet (SharePoint).

Recommendation 3

The Training Department should ensure that it is made clear to employees attending training as to what is expected in terms of them claiming for loss of earnings while attending training courses. This should be emphasised as an integral part of each training course.