BEDFORDSHIRE FIRE AND RESCUE AUTHORITY

Internal Audit Progress Report

14 July 2022

This report is solely for the use of the persons to whom it is addressed.
To the fullest extent permitted by law, RSM UK Risk Assurance Services LLP
will accept no responsibility or liability in respect of this report to any other party.

Contents

Progress against the internal audit plan 2021/22 & 2022/23

The Internal Audit Plan for 2022/23 was approved by the Audit & Standards Committee March 2022. Five audits have been finalised since the last meeting. The audits highlighted in bold have been finalised since the last meeting. Copies of the executive summaries and action plans are included as an appendix to this report.

Assignment and Executive Lead	Status / Opinion issued	Actions agreed			Planned Timing (as per ANA)
		L	M	H	
2021/22					
Data Quality to support the Community Risk Management Plan	Final Report – Partial Assurance	2	3	1	Q3
Debrief and Organisational Learning	**Final Report- Reasonable Assurance**	**2**	**2**	**0**	**Q2**
Key Financial Controls	**Final Report- Reasonable Assurance**	**6**	**2**	**0**	**Q3**
Management of Assets (Airwave Radios)	**Final Report- Reasonable Assurance**	**2**	**1**	**0**	**TBC**
Risk Management	**Final Report- Partial Assurance**	**0**	**5**	**0**	**Q2/3**
Human Resources – Grey Book Recruitment	**Final Report- Substantial Assurance**	**1**	**0**	**0**	**Q4**
Follow up	In Progress				Q4
2022/23					
ICT – Digitalised Systems User Proficiency	In Progress				Q1
Data Quality – Information Management and Governance Arrangements including GDPR	To commence 8 August 2022				Q1
Governance	To commence 15 August 2022 – see note below				Q2
Risk Management	To commence 24 October 2022 – see note below				Q3
Key Financial Controls	To commence 14 November 2022				Q3
Follow Up	To commence 6 March 2023				Q4

Other matters

Head of Internal Audit Opinion

The Audit and Standards Committee should note that the assurances given in our audit assignments are included within our Annual Assurance report. The Committee should note that any negative assurance opinions will need to be noted in the annual report and may result in a qualified or negative annual opinion. The Annual Report and Head of Internal Audit Opinion for 2021/22 is included as a separate agenda item.

Changes to the audit plan

The organisation is commissioning the LGA to conduct an independent review of governance and as such it is proposed that the days allocated for the review of governance, alongside some of the time allocated to risk management are utilised to review how the service engages with its local community to build a comprehensive profile of risk in its service areas following on from the issues identified in the HMICFRS report. The remaining time will be allocated to increase the follow up budget to include a more detailed follow up of risk management.

Information and briefings

We have issued the following client briefings since the last Audit & Standards Committee:

- Emergency Services News Briefing March 2022
- Emergency Services News Briefing June 2022

Quality assurance and continual improvement

To ensure that RSM remains compliant with the IIA standards and the financial services recommendations for Internal Audit we have a dedicated internal Quality Assurance Team who undertake a programme of reviews to ensure the quality of our audit assignments. This is applicable to all Heads of Internal Audit, where a sample of their clients will be reviewed. Any findings from these reviews being used to inform the training needs of our audit teams.

The Quality Assurance Team is made up of; the Head of the Quality Assurance Department (FCA qualified) and an Associate Director (FCCA qualified), with support from other team members across the department.

This is in addition to any feedback we receive from our post assignment surveys, client feedback, appraisal processes and training needs assessments.

Appendix A – Executive summaries and action plans from finalised reports (High and Medium priority actions only)

EXECUTIVE SUMMARY – DEBRIEF AND ORGANISATIONAL LEARNING

Why we completed this audit

As part of the approved 2021/22 annual audit plan for Bedfordshire Fire and Rescue Authority (the Authority), we have undertaken a review of the incident debrief processes and subsequent learnings, to assess the effectiveness and to provide assurance that learnings are being identified as well as taken on and embedded within subsequent processes.

A variety of debriefs are undertaken depending on a number of triggers including the incident type and number of pump vehicles in attendance. All incidents should have a 'hot debrief' undertaken on site at the time of the incident, and if required further 'cold' debriefs are undertaken where all details and outcomes are documented.

The Service introduced an Operational Assurance Department in December 2019 with one purpose being to improve the debrief and learnings processes. The department is led by the Head of Training and Assurance, supported by the Station Manager - Operational Assurance and Watch Commander – Operational Assurance. This department also works closely with the training and development team, with many outcomes of incidents being forwarded to them to incorporate into different training exercises.

There is an Assurance Working Group (AWG) in place, which reviews the information, data and learning generated within debriefs, with actions being discussed and agreed as relevant. Each action is risk rated by the group and placed onto a AWG action plan on the Service SharePoint site for tracking and implementation. In the event that concerns are identified within the AWG, these are escalated and discussed within the Service Delivery Leadership Team (SDLT) to ensure further expertise is sought and there is appropriate oversight.

National Operational Learning (NOL) and Joint Organisational Learning (JOL) action notes are received by the Single Point of Contact within the Service who uploads these onto a NOL and JOL action plan on the Service SharePoint site, assigning owners as relevant for tracking and implementation.

Conclusion

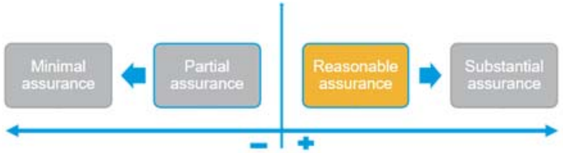
Our review found that in general there are robust controls that are complied with to ensure lessons, whether positive or negative learnings, are identified after an incident, and acted upon to ensure the change becomes part of standard process including a clear debrief templates, governance forums and lesson learnt.

We did note a few areas improvement, including a lack of notification to allow monitoring of completion of verbal hot debriefs, and trend analysis is not currently performed on incident data hampering the ability to understand and identify repeat issues or failings in embedding lessons.

Internal audit opinion:

Taking account of the issues identified, the Authority can take reasonable assurance that the controls upon which the organisation relies to manage this area are suitably designed, consistently applied and effective.

However, we have identified issues that need to be addressed in order to ensure that the control framework is effective in managing the identified area(s).



Key findings

We identified the following weaknesses resulting in the agreement of two medium priority action:

Assurance Working Group and SDLT Lessons Learnt and Trend Analysis

We obtained the previous January, April, and June 2021 Operational Debrief Working Group minutes but noted the meetings were restructured in April 2021 to become the Assurance Working Group.

Whilst we noted one instance of identifying lessons was demonstrated within the January 2021 meeting minutes, we noted the discussion of lessons learnt could not be evidenced within the April and June 2021 Assurance Working Group minutes. Where lessons learnt are not applicable this should be noted in the minutes to evidence that the forum is undertaking its responsibilities appropriately.

Furthermore, we were advised by the Station Commander – Organisation Assurance that trend analysis was not performed. This was further substantiated through review of the January, April, and June 2021 AWG meeting minutes and the SDLT January, May and July 2021 meeting minutes, where we noted the identification and discussion of incident trends could not be evidenced.

Without performing trend analysis and identifying lessons following incidents, there is a risk that issues and inefficiencies identified when responding to incidents may reoccur. This may hinder the safety of both operational staff and the public involved in incidents. Furthermore, without trend analysis there is no mechanism to assess the effectiveness of lessons implemented. **(Medium)**

Hot Debrief Recording

We selected a sample of 10 incidents where only a hot debrief would be required, and sought to gain assurance that these had been undertaken. However, we were unable to gain any assurance that these had occurred, as currently unless there are learnings (positive or negative) which are recorded in a further debrief form, the occurrence of the hot debrief is not noted.

In the absence of a tracking and monitoring process there is a risk that these are not occurring at every incident, which could result in the required feedback and reflection not occurring which could result in actions to improve performance and delivery. **(Medium)**

We noted the following controls to be adequately designed and operating effectively:

✓

Debrief Trigger Points

The Operational Debrief Policy does not explicitly define the trigger points for identifying the incident debrief procedure as 'Strategic', 'Tactical' or 'Operational'. There are however trigger points which determine the type of debrief(s) to undertake.

Through review of the draft Debrief Scheme Policy, we confirmed it clearly identified the types of debriefs to be conducted (hot debrief and cold debrief) and the debrief reporting types (informal and formal). Trigger points for each type of debrief to be followed were identified, assisting in ensuring the correct process is followed, and the right discussion taking place. The Station Manager - Operational Assurance also explained the function of the Operational Assurance Team in reviewing debriefs and determining how and where lessons should be shared. We also noted that the Operational Assurance meeting is a forum where these decisions can also be made as appropriate.

✓

Debrief Templates

To ensure debriefs are consistently completed, standardised debrief templates were developed.

Hot debrief:

We obtained a link to the Operational Hot Debrief form undertaken for relevant hot debriefs. We noted this provided a standardised layout where the key facts for the incident can be recorded easily within 24 questions. This includes basic incident information such as date, address, type, as well as further questions on the nature of the incident, as well as performance, planning, safety, inter-agency working and resource performance. We noted that where a question was answered negatively there was the requirement to provide further information to inform the reader.

Formal Incident debrief:

To support the formal Post Incident Debrief form template, we were advised that an Incident Debrief procedure was also formed. Through review of the procedure, we confirmed it provided a link to the Post Incident Debrief Form which is to be completed following an incident which triggers a formal debrief, which we noted was stored on a shared network drive. We found the procedure captured example incidents in which debriefs are to be completed.

Through review of the template, we found this was sufficiently detailed to allow the details of the incident to be documented for upload to the system. This includes information on those in attendance and what the incident entailed.

We also reviewed the Post Incident Debrief Assessment (PIDA) that is held on the Sphera-Cloud system and completed for formal debriefs. We found this covered the five key areas as above, with a range of questions on each topic, which also allows the completer to add further detail as necessary. We found the interoperability section appropriately detailed allowing an assessment on performance as well as whether there were any areas of good practice or potential development areas identified.

Control Debrief:

We reviewed the content of this form and noted it was clear covering the key areas allowing the Control Personnel to form a case and raise any concerns / lessons in a standardised structure.

Post Incident Structured Debrief:

The template of questions used by the Single Pont of Contact (SPoC) when undertaking these in person debriefs was obtained for review. We noted this was split into two key areas - areas of improvement and areas of good practice, as explained in the National Structured Debrief template developed by the College of Policing and recognised as best practice by the National Fire Chiefs Council.

Multi Agency Debrief:

The Service have developed their own Multi-Agency debrief form. We noted this broadly followed the National Structured Debrief template developed by the College of Policing. We compared this to the Joint Emergency Services Interoperability Principles (JESIP) Multiagency suggested template and noted the Service had pulled some key aspects from this to enhance their form ensuring the key principles were captured to ensure what worked and what did was clear with the JESIP principles an area for consideration.

✓ Assurance Working Group Functioning

The Group is responsible for the review of incident outcomes, the development of action plans, and the monitoring of such plans. Furthermore, lessons are to be identified following incidents. We obtained the agenda for this forum and noted it included a section on operational debriefs as well as NOL and JOL where learnings can be identified for sharing, or taken on by the Service as appropriate.

The terms of reference were included within the draft Debrief Scheme Policy and we found these to be adequately detailed setting out the role of the forum as well as meeting expectations and reporting lines. Provided the forum are aware of the detail within the policy, and it is reviewed annually, we do not believe there is a weakness in maintaining it in this manner.

Through review of the January, April, and June 2021 meeting minutes we noted action plans which we found captured key information as expected. We confirmed in all instances updates were consistently provided for the action plans against incidents and corresponding debriefs that had occurred and the corresponding actions raised. Furthermore, we noted incident and debrief updates were provided in succeeding meetings until actions were closed following implementation.

✓ Service Delivery Leadership Team Functioning

The Fire and Rescue Service has established a Service Delivery Leadership Team (SDLT) forum which monitors project performance and incidents that have occurred. In the event that concerns are identified within the Operational Assurance Group, they are to be escalated and discussed within the SDLT.

We obtained the January, May, and July 2021 SDLT minutes, and through review we confirmed that an operational debrief meeting update was presented within the January 2021 meeting minutes. As at January 2021, we noted 26 incidents were reported to the SDLT. Of the 26 incidents, we found in one case it was reported training was delivered in relation to an ammonia leak. This was further corroborated through review of the training material produced.

Through review of the May and July 2021 meeting minutes, we found no updates were reported to the SDLT regarding incident operational debriefs. As per the Assurance Working Group Terms of Reference (ToR), we noted decisions to be made and incident issues are to be reported to the SDLT on an exception basis only for further discussion only. As we noted neither were presented to the SDLT and have found incidents were reviewed in depth at an operational level (Assurance Working Group), we have not considered this to be an exception.

✓

Lessons Learnt

Lessons learnt from incidents (including NOL and JOL) and incident debriefs are disseminated via a range of methods including being uploaded onto LearnPro and via Operational Assurance Information Bulletins and Safety Flashes. Information is retained on LearnPro for a maximum of six months while it is incorporated into guidance / learning so that it becomes business as usual. We reviewed the LearnPro site and noted bulletins loaded which were easily accessible from the home page. We reviewed the safety flashes section for ease of access, however noted there are no active safety flashes, with the most recent safety flash being dated November 2020.

We selected a sample of five safety flashes / bulletins to assess how these lessons had been shared and embedded. In all five cases we were provided with the original bulletin / flash and noted this included the key points of learning, including further actions to be undertaken to embed the learnings. We found these further actions ranged in type including incorporating into policy, including in training exercises and incorporating into online learning assessments. For our sample of five we also confirmed that the further actions identified had been implemented, and the learnings had been embedded and made business as usual.

We were informed that when a user logs in to LearnPro a message will pop up to alert them that there is a new bulletin or safety flash. They are required to tick a box to confirm they have read the alert, and can then review the detail of the case. Assessments are also required to be completed to ensure they have read and understood the content. We obtained the LearnPro report for four of the safety notices in our sample of five. We were informed that there was no assessment question bank created for the fifth dated 2018, however personnel were asked to read the safety flash and enter on their electronic training record that this had been read.

The remaining four reports included the detail on whether staff have completed and passed a mini assessment which relate to the safety flash / bulletin. We noted that completion rates stood at 62 per cent (2015), 68 per cent (2017), 74 per cent (2018) and 86 per cent (2020). We were informed by the Digital Learning Coordinator that as the reports provided were being run recently on old assessments, the number of completions were being artificially pushed down as any new personnel would not be required to sit the assessment as it would not be available to them however their name would still be in the report and marked by a non-completion.

The training and development team run reports on safety flash assessment completion usually after a month to coincide with Operational Development Team (ODT) meetings so that they can raise those who are outstanding to line managers. Further chasing up if required is also done by the Health and Safety team via email. We obtained an example of ODT minutes where we can see a report was presented and the number outstanding highlighted.

Cold Debrief Completion

As per the Debrief Scheme Policy, debriefs are to be completed following incidents. However, the types of debriefs to be conducted vary upon incident type. A report of all incidents from April 2021 to September 2021 was obtained, and we selected a sample of 10 complex incidents to confirm that the correct debriefs were performed, these were timely, those involved were documented and learnings were identified and disseminated as appropriate.

We found that six of our sample of ten did not require formal debrief reporting, and were satisfied with the explanations for why these did not occur, including mobilising exercises and false alarms. In four cases we found that a formal debrief was undertaken and logged with a debrief form provided as evidence. We found that those involved were documented and involved in the debrief as required, however we found in no case was the debrief completed by all required individuals within the two weeks required.

We further discussed this with the Station Manager - Operational Assurance and were informed that the system sends a reminder at two weeks that a debrief requires completion, the Operational Assurance team track and chase outliers (as evidenced through review of their tracker), and Line Managers are informed of non-completion. We also noted that the two week expectation was clear within the draft policy. To provide assurance on the processes we reviewed the tracking spreadsheet and noted that between June and September 2021 there were no individuals where a debrief was still awaited so although not always timely they are being completed. We also found that the majority of respondents were within the two week timeframe ensuring accurate accounts and fresh memories were being shared to assist in the debrief and learning process.

National Operational Learning (NOL) and Joint Organisational Learning (JOL) action plan

A NOL and JOL action plan is maintained which logs NOL and JOL action points, tracking implementation of required changes to the Services processes. We performed a walkthrough of the action log noting this was on a SharePoint site with access for relevant individuals to update and make changes as required.

It was explained that this action plan came into effect on 1 October 2021. As such there is only one live action, however legacy actions were transferred across from the old spreadsheet used to track implementation to ensure the audit trail for these is retained in one central location.

The SPoC explained that they receive notifications on NOL and JOL action points to their email and upload these into the action plan. They then assign individuals to complete the action as appropriate, and monitor them through to completion. Once assigned the action plan automatically emails the owners with details of the action and required outcomes. We reviewed a recent example and noted the action point that had come in, the addition to the action plan, as well as the email sent out by the responsible owner alerting the SPoC to progress.

We have agreed a further **two low** priority management actions, the details of which can be found in section two of this report.

2. DETAILED FINDINGS AND ACTIONS

This report has been prepared by exception. Therefore, we have included in this section, only those areas of weakness in control or examples of lapses in control identified from our testing and not the outcome of all internal audit testing undertaken.

Assurance Working Group Lessons Learnt and Trend Analysis		
Control	To support the management of debriefs and organisational learning, the Fire and Rescue Service has established an Operational Debrief Working Group (ODWG) which became the Assurance Working Group from April 2021. The Group is responsible for the review of incident outcomes, the development of action plans, and the monitoring of such plans. Furthermore, lessons are to be identified following incidents. Per the draft policy “the operational debrief schemes will enable the Service to audit and review using historical data on not only those incidents which have occurred since the previous debrief working group meeting, but also to identify trends or areas of high reporting on the same issue over a longer period. This trend information will be reported to SDLT twice a year to highlight common themes and the action taken to improve these areas".	**Assessment:** **Design** ✓ **Compliance** ×
Findings / Implications	We obtained the previous January, April, and June 2021 Operational Debrief Working Group minutes but noted the meetings were restructured in April 2021 to become the Assurance Working Group. We noted the meeting minutes provided consisted of action plans which we found captured key information which included: - incidents that occurred; - brief details; - actions agreed; - action due dates; - risk and national risk ratings. Through review of the action plans, we confirmed in all instances updates were consistently provided against incidents and corresponding debriefs that had occurred and the corresponding actions raised. Furthermore, we noted incident and debrief updates were provided in succeeding meetings until actions were closed following implementation. Following an incident that was reported within the January 2021 meeting, we noted an opportunity for a lesson learnt was identified and subsequently formed. Through review of the action updates, we noted the lesson was shared with external agencies involved with the incident [F2042884]. Whilst we noted one instance of identifying lessons was demonstrated within the January 2021 meeting minutes, we noted the discussion of lessons learnt could not be evidenced within the April and June 2021 Assurance Working Group minutes. We were advised by the Station Commander – Organisation Assurance that trend analysis is not currently performed. This was further substantiated through review of the January, April, and June 2021 AWG meeting minutes where we noted the identification and discussion of incident trends could not be evidenced.	

Assurance Working Group Lessons Learnt and Trend Analysis

Without performing trend analysis and identifying lessons following incidents, there is a risk that issues and inefficiencies identified when responding to incidents may reoccur. This may hinder the safety of both operational staff and the public involved in incidents. Furthermore without trend analysis there is no mechanism to assess the effectiveness of lessons implemented.

Management Action 2	The Station Commander – Organisation Assurance will reiterate the importance to management of identifying lessons learnt during Assurance Working Group meetings. Where lessons learnt are not applicable, this will be clearly stated within meeting minutes against the incident under review. Furthermore, the Station Commander will collate all incidents reported to facilitate the analysis of trends. Incident trends will be actively reported and discussed within meetings.	**Responsible Owner:** **Steve Frank, Headf of Strategic Support and Assurance (HSSA)**	**Date:** **July 2022**	**Priority:** Medium

Hot Debrief Completion

Control

Hot debriefs are to be completed on site following all incidents. Where the incident is classed as a small incident, this is the only debrief required.

These are generally verbal updates, although if there are any learnings or best practice coming out of an incident this can be recorded on an electronic hot debrief form.

Assessment:

Design	✓
Compliance	×

Findings / Implications

A report of all incidents from April 2021 to September 2021 was obtained and we selected a sample of 10 incidents where only a hot debrief would be completed. We sought to gain assurance that these had been undertaken, however we were unable to gain any assurance that these had occurred, as currently unless it is felt necessary to record information (e.g. good practice, issues etc) the occurrence of the hot debrief is not noted.

In the absence of a tracking and monitoring process there is a risk that these are not occurring at every incident, which could result in the required feedback and reflection not occurring which could result in actions to improve performance and delivery not being undertaken.

Management Action 3

The Service will consider implementing a method to track the occurrence of hot debriefs to ensure these are happening as required, and allowing trend analysis of the output of data. To allow this the addition of a 'Hot debrief conducted' field to the stop message to control will be considered.

Responsible Owner:	**Date:**	**Priority:**
Steve Frank, Headf of Strategic Support and Assurance (HSSA)	**December 2022**	Medium

EXECUTIVE SUMMARY – KFC ACCOUNTS PAYABLE AND GENERAL LEDGER

Why we completed this audit

As part of the approved 2021/22 annual audit plan for Bedfordshire Fire and Rescue Authority (the Authority), we have undertaken a review of key financial controls, focusing on general ledger and accounts payable. The purpose of this was to allow management to take assurance that the finance system is appropriately managed to ensure that all financial transactions are accurately recorded, and appropriate payments are made.

The Authority uses the Great Plains finance system to record its financial transactions, including general ledger and accounts payable. The finance system is backed-up by the ICT Shared Services Team for the Bedfordshire and Cambridgeshire Fire and Rescue Authorities. The Authority has established a prompt payment target for its accounts payable invoices, aiming to pay 96 per cent of uncontested invoices within 30 days of receipt. Performance against this target is reported to the Authority each quarter.

As part of this review, we have also performed data analytics on overtime claims paid in 2021/22 to date, to identify instances of non-compliance with the Authority’s Pay Policy regarding overtime payments, with follow up testing completed to further investigate potential exceptions identified from this, further details can be found later in our report.

Conclusion

Our review identified issues requiring management attention, resulting in the agreement of two medium priority management actions. We identified that the Authority’s finance system was not scheduled to be backed up at an appropriate frequency, risking data loss, whilst we also noted that back-ups had not been routinely completed at the current frequency required. In addition, we identified issues regarding overtime being paid at rates below those due to the relevant staff member, due to a lack of scrutiny by the approver. Further issues were identified resulting in six low priority actions being agreed, including prompt payment targets not being met, finance system access not being removed in a timely manner for leavers and purchase orders being raised retrospectively.

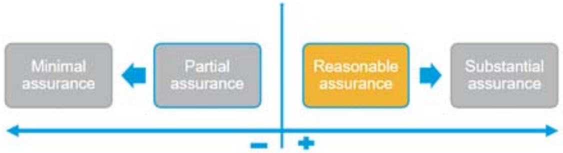
We did, however, find that the Authority had appropriate controls in place, which were well designed and operating effectively, governing key processes including supplier set-ups and detail amendments, raising of purchase orders, payment of invoices and payment runs, raising of journals and changes to the chart of accounts, including appropriate approvals and segregation of duties. For requisitions and invoices, we noted that an authorised signatory list was in place, which was subject to regular and controlled update, detailing the approval limits assigned to all authorisers.

In addition, we confirmed that control account reconciliations were being completed and approved in a timely manner for each month, whilst the trial balance is also reviewed monthly to ensure that this balances. We also noted that training plans are in place for new finance staff to familiarise them with key processes.

Internal audit opinion:

Taking account of the issues identified, the Authority can take reasonable assurance that the controls upon which the organisation relies to manage this risk are suitably designed, consistently applied and effective.

However, we have identified issues that need to be addressed in order to ensure that the control framework is effective in managing the area.



Key findings

We identified the following weaknesses resulting in the agreement of two medium priority actions:

Finance System Back-ups

We confirmed from screenshots of backup logs that Great Plains had been backed-up monthly between August and October 2021. However, we noted that evidence was not provided that weekly back-ups were being routinely performed, with evidence of weekly backups only provided for three out of 12 weeks between 30 August and 21 November 2021. Subsequent to the audit we were provided with evidence to demonstrate that weekly back-ups of Great Plains had been successfully completed between 31 January 2022 and 28 February 2022.

In addition to this, we noted that the Authority's current weekly back-up for its finance system was not in line with standard practice, as the completion of weekly back-ups still risks up to a week of financial data required for financial accounts being lost even when back-ups are being performed routinely each week. If the finance system is not backed-up routinely at an appropriate frequency, there is a risk that the Authority may be unable to restore its finance system to the desired recovery point when required, risking inaccuracies in financial data when transactions are recreated. **(Medium)**

Overtime

Via data analysis on a report of all overtime claims paid in 2021/22 and subsequent follow up testing, we identified issues relating to overtime being paid at incorrect rates, due to rates being entered incorrectly by the claimant, and not being sufficiently scrutinised by the respective approver. Whilst all instances identified resulted in the member of staff receiving less than the actual amount due, there is a risk that this could affect budget monitoring processes where additional overtime payments need to be made in subsequent months to correct the overtime rates paid to these staff. In addition, there is a risk of overtime claims being paid at a rate above or below what is owed by the Authority if claims are not appropriately scrutinised. **(Medium)**

We noted the following controls to be adequately designed and operating effectively:

✓ New Suppliers and Supplier Detail Amendments

For a sample of 10 suppliers set up since April 2021, we confirmed that in each case the set-up was appropriately requested and approved, with bank details obtained on letter headed paper or via an appropriate alternative. In addition, we confirmed that a New Creditor Card Form was completed for all ten set-ups, with the set-up appropriately verified, before being validated by a second member of the Finance Team and checked by a third member following an alert from Great Plains. In each case, we confirmed that the supplier had been set-up accurately on Great Plains.

Similarly, for a sample of nine supplier detail amendments processed since April 2021, we confirmed that in each case, the amendment had been appropriately requested or identified, and had then been verified using an appropriate method, with a Creditor Card Change Form completed. We noted that in each case, the amendment had been checked by a second and third member of the Finance Team and was processed accurately.

✓ Delegation of Authorities

Through review of the Financial Regulations, we noted that these detailed responsibilities and authorisation limits which had been delegated to the Chief Fire Officer/Chief Executive and the Treasurer by the Authority, for key areas including write offs, virements and the capital programme, as well those retained by the Authority itself.

✓ Authorised Signatory List

We confirmed that authorised signatory lists were in place detailing the staff who can approve requisitions and invoices and their respective approval limits and noted that these had been subject to regular update as required throughout 2021/22 to date. Via sample testing of five authorisers who had been added to the authorised signatory list or whose approval limit had been altered in 2021/22, we confirmed that appropriate mechanisms were in place to process both types of changes, with new staff added to the authorised signatory list when appointed to a vacant position with a corresponding authorisation limit, and limits updated for existing authorisers following request and appropriate approval.

✓ Approval of Purchase Orders and Invoices

We selected a sample of 20 invoices paid since April 2021 for which a corresponding purchase order was raised. In each case, we confirmed that a purchase order had been requested and approved, with the purchase order approved by an authorised signatory with a sufficient approval limit. In each case, we also noted that there was segregation of duties between request and approval of the purchase order.

In addition, we confirmed that all 20 invoices were approved by an authoriser from the relevant department with an authorisation limit greater than the invoice value, to confirm that goods/services had been received and that the invoice should be paid, with all invoices approved prior to payment.

✓ Non-PO Invoices

Via sample testing of ten non-PO invoices processed in 2021/22, we confirmed that non-PO invoices were being used in appropriate scenarios, either for payments where raising a purchase order was not practical/necessary, or for other purposes such as to process payroll pay-overs or clear suspense accounts. In addition, where actual payments were made for these invoices, we confirmed that the invoice had been appropriately approved for payment by an authoriser on the authorised signatory list with a sufficient authorisation limit.

✓ Payment Runs

We confirmed that supplier payment runs had been completed for a sample of five weeks, and in each case, we noted that the payment run had been prepared by the Principal Finance Officer and approved prior to submission by the Chief Accountant. For each payment run in our sample, we noted that the total submitted for payment matched to supporting documentation, and that the amount paid per the Authority’s bank statement matched the amount that was authorised and submitted. We also noted that all payments over £50,000 were initialled by the Chief Accountant to confirm approval.

✓ Financial Regulations

Through review of the Financial Regulations, we found that these were last updated in March 2021, and confirmed from meeting minutes that these were approved by the Audit and Standards Committee in March 2021. We also confirmed that these were available on the Authority’s website. In terms of content, we noted that the Regulations detailed the high-level responsibilities of key staff regarding accounting and financial controls.

✓ Finance System Users

We were provided with reports of Great Plains users. Through comparison of this to the equivalent reports from the 2020/21 Key Financial Controls Audit, we identified 4 users who were set-up on Great Plains since the previous audit. In one case, we noted that the user account was a test account for a current member of the IT department, and as such a request form was not required. In the remaining three cases, we confirmed that an Access Request Form had been completed for the user detailing their need for access, which had been appropriately approved.

We also selected a sample of five active users of Great Plains from the above report. In all five cases, we were advised by the Principal Finance Officer that the member of staff was currently employed at the Authority, and that their level of system access was appropriate for their role.

✓ Finance Training

We were informed by the Chief Accountant that there had been one starter in the Finance Department since April 2021. For this starter, we confirmed that a training plan was in place detailing the finance processes on which they were to receive training and the period over which this training would be provided, and we noted that completion of this training was being recorded on the plan to monitor the progress made.

Month-end Checklist

We were provided with the month-end checklists for June, July and August 2021, and noted that in each case, this detailed key tasks to be completed, the person responsible and the deadline for completion.

Chart of Accounts

We selected a sample of ten account codes set up in 2021/22 and confirmed that each had been appropriately requested and approved.

Journals

For a sample of 20 journals posted in 2021/22 to date, we confirmed that in each case the journal had been originated via an appropriate form, the journal balanced, and appropriate narrative and supporting information was provided. In 17 cases, we noted that the journal was originated by a member of the Finance Team and then approved by the Chief Accountant. In the final three cases, we noted that the journal was originated and approved by the Chief Accountant, due it's technical nature, although it had been checked by a second member of the Finance Team.

Control Account Reconciliations

We confirmed that monthly control account reconciliations were completed for June to September 2021 for accounts payable, accounts receivable and bank accounts. In each case, we confirmed that the relevant control account and sub-ledger/bank accounts were reconciled to a difference of zero, with the balances used matching to supporting information. In each case, we confirmed that the reconciliation was prepared in a timely manner and was then reviewed and signed off in a timely manner by the Principal Finance Officer.

Review of the Trial Balance

We were provided with the revenue budget variance calculations for September and October 2021. Through review of these, we noted that as part of this work, a check had been performed on the trial balance for the month, to ensure that the debits and credits balanced to zero, which was the case in both months. We noted that the checks for both months had been performed within 2 weeks of month end, enabling timely rectification of errors.

We have agreed a further **six low** priority management actions, the details of which can be found in section two of this report, as well as two best practice recommendations, detailed in Appendix B of the report.

2. DETAILED FINDINGS AND ACTIONS

This report has been prepared by exception. Therefore, we have included in this section, only those areas of weakness in control or examples of lapses in control identified from our testing and not the outcome of all internal audit testing undertaken.

Finance System Back-ups				
Control	Data from Great Plains is backed-up on a weekly basis by the ICT Shared Services Team for Bedfordshire and Cambridgeshire Fire and Rescue Authorities, with full back-ups completed every Friday. In addition, a monthly back-up of Great Plains is performed at the end of each month. However, the current back-up schedule does not include incremental back-ups or snapshots in the seven-day period between full backups being performed. As such, the Authority is exposed to up to seven days of data loss from its finance system even when backups are being consistently performed at the required frequency.	**Assessment:** **Design** × **Compliance** N/A		
Findings / Implications	We confirmed from screenshots of backup logs that Great Plains had been backed-up on a monthly basis in the period from August to October 2021. However, we noted that weekly back-ups were not being routinely performed over this period, with weekly backups only evidenced for three out of 12 weeks between 30 August and 21 November 2021. Subsequent to the audit we were provided with evidence to demonstrate that weekly back-ups of Great Plains had been successfully completed between 31 January 2022 and 28 February 2022. If back-ups are not completed at the agreed frequency, there is a risk that the Authority may be unable to restore its finance system to the desired recovery point in the event of a cyber incident, resulting in data loss. In addition to this, we noted that the Authority's current back-up frequency for its finance system was not in line with standard practice, as the completion of weekly back-ups still risks up to a week of financial data being lost even when back-ups are being performed routinely each week. As the Authority relies on data from its finance system for its financial accounts, the loss this quantity of data will result in considerable time and effort to ensure all transactions over the period where data has been lost are accurately recreated within the finance system, risking inaccuracies in financial data.			
Management Action 6	The Authority will liaise with the ICT Shared Services Team to implement a process whereby incremental back-ups of the finance system are completed daily, with full back-ups completed weekly and monthly. If daily back-ups are not implemented, this will be reported to the Audit and Standards Committee, and the associated risk will be formally accepted by the Committee.	**Responsible Owner:** **Jeremy Harrison, Chief Accountant**	**Date:** December 2022	**Priority:** Medium

	Once the revised frequency has been agreed, the finance system will then be periodically backed-up in line with this, with evidence of this clearly retained.			

Data Analytics: Overtime Rates

Findings / Implications	Through analysis of overtime payments paid by the Authority in 2021/22 to date, we identified 41 instances out of 1194 claims where the overtime was worked on a weekend, but the rate paid was not in line with the standard weekend rates of time and a half for Saturday or double time for Sunday. We selected 20 of these claims, and noted that in eight instances, there was an appropriate reason for the claim being paid at an alternative rate, for example where the overtime related to a voluntary role as part of the vaccination programme. However, in the remaining 12 cases, we noted there was no clear reasoning for the claim to be paid at the alternative rate, and as such that the date of the overtime or the required rate had been input incorrectly on iTrent by the member of staff submitting the claim, despite the correct rates being highlighted in iTrent. We noted that one of the reasons why it was not possible to verify if the rate for these exceptions was correct was that it is not currently mandatory for a reason to be provided with the overtime claim. Without this information being recorded, it will not be possible for managers to appropriately review overtime claims for legitimacy and accuracy. In addition, the above exceptions demonstrate non-compliance with the need for authorisers to review the details of the claims they are approving, as the entry of incorrect rates was not identified. Although we noted that all of the potential exceptions identified by our data analysis involved a lower overtime rate than the standard rate owed, there is a risk that this could affect budget monitoring processes where additional overtime payments need to be made in subsequent months to correct the overtime rates paid to these staff. In addition, there is a risk of overtime claims being paid at a rate above or below what is owed by the Authority if claims are not appropriately scrutinised.			
Management Action 8	The need to include a description of the reason why overtime was performed as part of the comments section of the claim form will be made a mandatory requirement. This will be communicated to staff, along with a reminder of the correct rates to claim and the need for approvers to review claims in sufficient detail to ensure that rates are correct, and that reasoning has been recorded. The Payroll Team will periodically review all overtime claims made to ensure that the reason for the claim is being recorded, with action taken to address repeated instances where this is not recorded. Consideration will also be given as to whether data analysis can be used to identify claims paid at non-standard rates, with these investigated to ensure that this was appropriate.	**Responsible Owner:** **Jeremy Harrison, Chief Accountant**	**Date:** December 2022	**Priority:** Medium

APPENDIX B: BEST PRACTICE RECOMMENDATIONS

During this audit, we identified a number of areas where controls were generally well designed and complied with, but where further improvements could be made in order for the Authority to meet standards of best practice. These areas are summarised below, along with recommendations for how these controls can be improved:

Control	Area identified for improvement	Recommendation
Month-end Checklists	Whilst we confirmed that a month-end checklist was in place and was being highlighted to mark tasks as complete, we identified instances on the checklists for June, July and August 2021 where tasks were not marked as complete, with no reasoning documented, although we were advised by the Financial Controller that these tasks no longer need to be completed. Furthermore, we noted that the checklist is not reviewed and signed off to ensure that all tasks have been completed as required. As such, there is currently a risk that month end tasks are not being completed in a timely manner, which could lead to errors within internal financial reports.	The month end checklist will be updated to remove all tasks which are no longer performed. Following this the revised checklist will be fully completed each month, with each task either marked as complete or non-completion noted along with reasoning. Once fully complete, the checklist will be reviewed and signed off as confirmation that all tasks have been completed as required and in a timely manner.
Control and Suspense Account Reconciliations	Through review of the monthly accounts payable, accounts receivable and suspense account reconciliations for June to September 2021, we confirmed that the approver of the reconciliation was clearly detailed in all cases, with all reconciliations approved by a Principal Finance Officer. However, we noted that the preparer was not clearly documented, although finance system screenshots used in the reconciliations evidenced that these had been obtained by a second member of staff. As such, we were unable to confirm that there was a clear segregation of duties between preparation and review of the reconciliations. Without this, there is a risk that errors in preparation of the reconciliation may not be identified.	We will ensure that the preparers of the accounts payable, accounts receivable and suspense account reconciliations are clearly documented each month, to evidence segregation of duties, along with the date of preparation.

EXECUTIVE SUMMARY – MANAGEMENT OF ASSETS (AIRWAVE RADIOS)

Why we completed this audit

This audit was completed to allow the Authority to take assurance that appropriate processes are in place to manage the Airwave radios which it has deployed and held in stores, and ensure that these are appropriately identified, recorded and tracked, to mitigate the risk that the Authority fails to effectively manage these radios.

The Airwave radio system operates on the Airwave network, and is the primary means of communication between the three emergency services, providing a secure means of communication between mobile resources, control rooms and across the three services. The Airwave network is commissioned and governed by the Home Office, and is managed by Motorola, whilst maintenance of the Authority's Airwave radios is carried out by Telent, an external contractor. The Airwave network is scheduled for replacement by the Emergency Services Network based on 4G LTE technology, however the implementation of this network has been delayed until 2024, having previously been scheduled for the end of 2022 on the updated timetable.

The Home Office requires the Authority to appoint a Custodian and Deputy Custodian, who act as points of contact with the Home Office and ensure that processes are in place to securely use and effectively manage Airwave radios. These roles have been held by the ICT Service Delivery Manager and ICT Support Manager since June 2021, when responsibility for managing these Airwave radios was transferred to the ICT Team. The ICT Team maintains an Airwave Asset Register, upon which it records the details of the Airwave radios which it holds including their serial number and the location or registration of the vehicle the radio is held in. An annual TEA2 audit is completed by the Home Office, with the information from the Authority's Register checked for accuracy against the records of the Home Office.

Conclusion

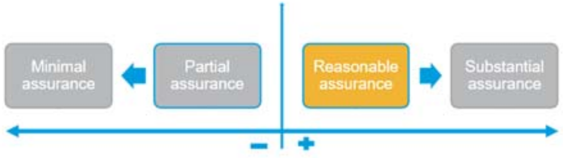
Our review identified that the Authority has well designed controls in place to record and manage its Airwave radios which are generally complied with. We noted that an Airwave Policy and Procedure was in placing, detailing the key processes for managing these radios, and that this document also stated the responsibilities of the Custodian and Deputy Custodian and assigned these roles to the ICT Service Delivery and ICT Support Managers. We also confirmed that an Airwave Asset Register was being maintained, with access to this appropriately restricted, and that the Authority had submitted an extract from this to the Home Office in a timely manner as part of it's TEA2 audit for 2022, with the Home Office confirming that this audit had been completed to a satisfactory standard. Furthermore, we confirmed that spare radios are being stored within a safe, and that the number and type of radios held in the safe matched to the Authority's Register.

However, we noted that the Authority does not currently have a systematic and evidenced process in place to periodically verify the location or vehicle which Airwave radios are held in. We also identified radios on the Asset Register which had no documented vehicle or user, whilst we also noted that the ICT Team does not maintain a log of radio installations and transfers, to provide a clear audit trail of changes in the location and user which a radio is assigned to.

Internal audit opinion:

Taking account of the issues identified, the Authority can take reasonable assurance that the controls upon which the organisation relies to manage this risk are suitably designed, consistently applied and effective.

However, we have identified issues that need to be addressed in order to ensure that the control framework is effective in managing the area.



Key findings

We identified the following weaknesses resulting in the agreement of one medium priority action:

Verification Processes and Stock Checks

We were informed by the ICT Support Manager that an audit was performed in June 2021 to verify the documented location or vehicle for all Airwave radios. Whilst no evidence of this process was maintained, we noted that the Airwave Asset Register had been developed based on this process. With regards to subsequent verification checks, the ICT Support Manager advised us that ad-hoc spot checks are completed to verify that radios are held in the documented location or vehicle per the Airwave Asset Register when ICT staff work on-site, whilst stock checks are completed approximately quarterly, to ensure that the spare radios held in the safe match to the Register.

The Airwave Policy and Procedure states that further audits are to be completed every six months, however, there is no evidence of these to demonstrate that they have occurred, and we identified that the current verification processes are not performed in a systematic manner to ensure that all devices are routinely checked at an appropriate frequency. We noted that the number and location of the Authority's Airwave radios is largely static, and misappropriation would likely be detected due to the operational importance of the radios as the main form of communication across the Emergency Services. However, there is a risk that the Authority's Airwave Asset Register may become inaccurate without periodic and systematic verification processes, resulting in the Authority failing to meet the Home Office's requirements. **(Medium)**

We noted the following controls to be adequately designed and operating effectively:

Airwave Policy and Procedure

We were provided with the Authority's Airwave Policy and Procedure, and noted that this was finalised in June 2021, and was therefore up to date. We were advised by the ICT Support Manager that formal approval of this guidance was not required, but that this had been agreed by the Airwave Radio Group. We confirmed via screenshot that the Policy and Procedure was available to staff on the Intranet and noted that this had been assigned a next review date of April 2022 on the Intranet by the Authority's Governance Team. We noted from a calendar screenshot that the ICT Support Manager had scheduled review of the Policy and Procedure for 5 April 2022, in line with this review date.

In terms of content, we confirmed that the Policy and Procedure provided guidance on key processes including the secure handling of Airwave radios, the transfer of radios between vehicles, reporting and management of lost and stolen radios and audits to verify the location radios.

Custodians

Through review of the Airwave Policy and Procedure, we confirmed that the roles and responsibilities of key staff and teams involved in the management of Airwave radios were clearly detailed. In addition, we confirmed that the roles of Airwave Custodian and Airwave Deputy Custodian had been clearly assigned to the ICT Service Delivery Manager and the ICT Support Manager within the Policy and Procedure, with the responsibilities associated with these roles clearly detailed.

Access to the Airwave Spreadsheet

We confirmed via screenshot that the Airwave Asset Register was available to relevant staff via the Sharepoint for the Airwave Radio Group, with 26 members of staff able to access this at the time of the audit. Of these, we noted that the ability to edit the Register was restricted to three appropriate members of staff, with the remaining staff only having read only access, preventing this from being edited by inappropriate staff members.

TEA2 Audit

Through review of email correspondence, we confirmed that the Authority had submitted its TEA2 audit return for 2022 to the Home Office in a timely manner on 2 February 2022, ahead of the deadline of 7 February 2022. We noted that the submission had been made by the ICT Support Manager in their role as Deputy Custodian, with the ICT Service Delivery Manager copied into the submission as the Custodian. As part of this submission, we confirmed that the Authority had provided the Home Office with an extract from the Airwave Asset Register detailing the serial number, status and the location or vehicle which the radio was assigned to, in order for them to verify this information against their own records.

Through review of further email correspondence from the Home Office, we noted that the Home Office had stated that the Authority's TEA2 audit for 2022 had been a 'perfect audit', and that they had closed the audit off after providing one recommendation to the Authority, which we confirmed had been actioned through review of the Airwave Asset Register.

Storage of Spare Radios

Through review of the Airwave Policy and Procedure, we noted that this clearly stated that spare Airwave radios must be stored securely, and the ICT Support Manager advised us spare radios were currently stored in a safe within a secure equipment storage room, which we confirmed via photograph. We noted from the photograph that eight spare radios were held in the safe, comprising of six handheld radios and two mounted radios. Through review of the Authority's Airwave Asset Register, we confirmed that the number and type of radios held in the safe agreed to the Register.

We have agreed a further **two low** priority management actions, the details of which can be found in section two of this report.

2. DETAILED FINDINGS AND ACTIONS

This report has been prepared by exception. Therefore, we have included in this section, only those areas of weakness in control or examples of lapses in control identified from our testing and not the outcome of all internal audit testing undertaken.

3. Verification Processes and Spot Checks

Control

The ICT Team completed a full audit of all radio locations in June 2021 when taking over responsibility for managing these radios, to ensure that accurate records were in place. Separate documentation was not maintained for this exercise, however, this was used to generate the Authority's Airwave Asset Register.

Whilst the Airwave Policy and Procedure states that further audits are to be completed every six months, a formal audit process has not been introduced to ensure that this requirement is complied with. Instead, the ICT Team currently verify that radios are in their documented location either when the Team attends a location or if an appliance comes into the stores for maintenance, however, no documentation is maintained to evidence these checks. Similarly, a quarterly check is done to ensure that the spare radios held in the safe at Headquarters match to the Airwave Asset Register, but no records of these checks are maintained.

To date, these processes have not identified discrepancies, however, any identified discrepancies would be documented and reported as required.

Assessment:

Design	×
Compliance	N/A

Findings / Implications

We were advised by the ICT Support Manager that a full audit of all Airwave radios had been completed in June 2021 to confirm where each device was located, following the ownership for the radios being transferred to the ICT Team. Whilst no evidence had been maintained from this audit, the ICT Support Manager advised us that this audit was the basis of the current Airwave Asset Register.

With regards to subsequent verification checks, the ICT Support Manager advised us that the following checks are completed:

- Ad-hoc spot checks are completed to verify the documented location or vehicle and user of radios when ICT staff are on-site or if a vehicle is returned to stores for maintenance.
- stock checks are performed approximately quarterly, to ensure that the spare radios held in the safe match to the Authority's records.

However, no documentation is retained for either of these processes to provide evidence that these checks have occurred and that no exceptions were identified, although the ICT Support Manager advised us that no exceptions had been identified by these processes, and that if any were to occur, they would be appropriately investigated and escalated to the Head of ICT. In addition, we noted that the current verification processes are not performed in a systematic manner to ensure that all devices are routinely checked, whilst we also noted that all devices are not being checked every six months, a requirement stated in the Airwave Policy and Procedure. We were advised by the ICT Support Manager that they had intended to introduce a systematic and evidenced verification process, but that this had not yet been possible due to a lack of available staff and the prioritisation of other work.

	We noted that the number and location of the Authority's Airwave radios is largely static, and that these radios are essential for operations, as they are the primary means of communication for the three emergency services, minimising the risk of these radios being misappropriated without identification of this. However, without periodic and systematic verification checks on the location of all Airwave radios, there is a risk that the Authority's Airwave Asset Register could become inaccurate, resulting in the Authority failing to meet the Home Office's requirement to maintain an accurate asset register which accounts for all terminals at all times.			
Management Action 3	The Authority will introduce a systematic and periodic verification process for Airwave radios which have been deployed, with physical checks performed to verify the documented location or vehicle and user (where relevant) of all radios at an appropriate frequency. Documentation will be maintained to evidence that this process is being completed and that all radios have been checked, with similar evidence maintained for the periodic stock check process performed for spare radios. Where radios are found to not be in their documented location, this will be investigated and reported as required, with the Register updated to reflect the correct asset location. These revised processes will be documented within the Airwave Policy and Procedures.	**Responsible Owner:** **Jason Tai, Head Training and Asset Management**	**Date:** December 2022	**Priority:** Medium

EXECUTIVE SUMMARY – RISK MANAGEMENT

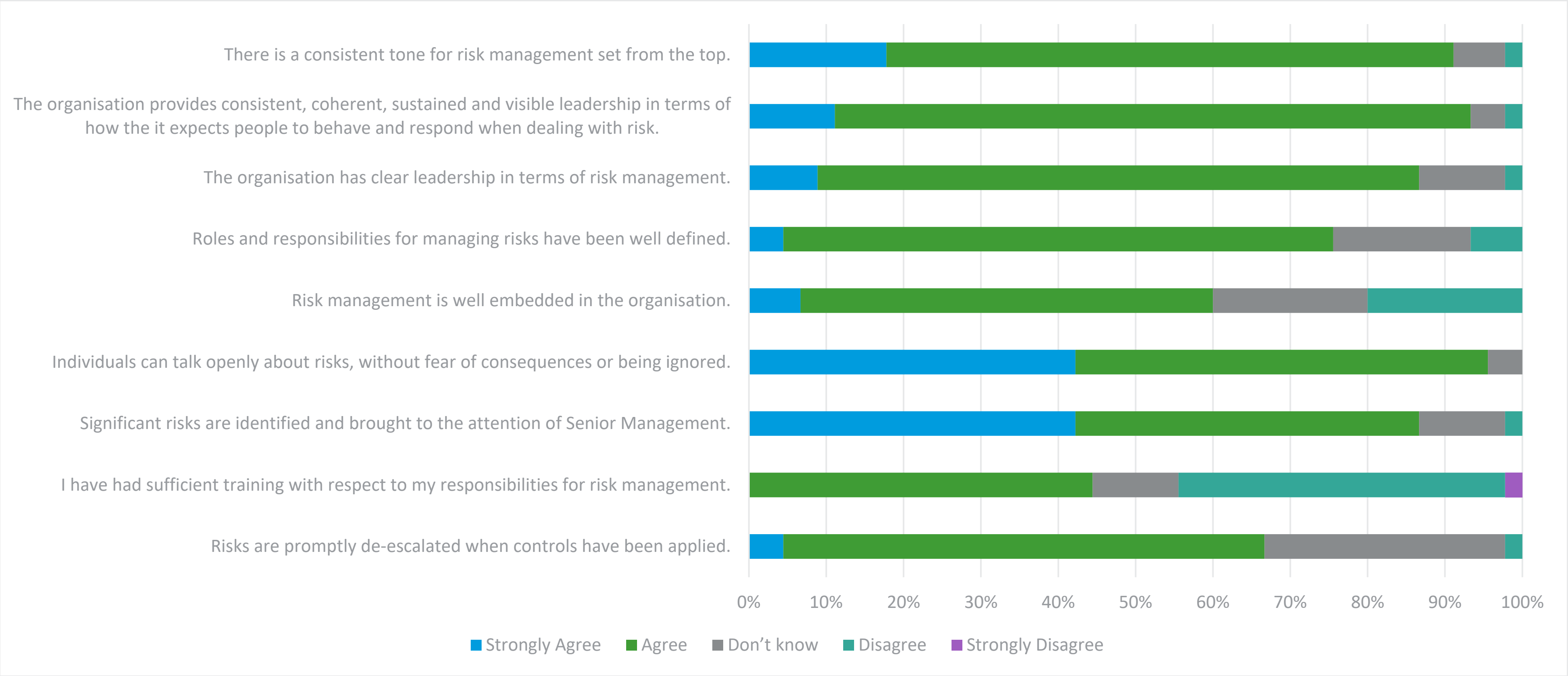
Why we completed this audit

We have undertaken a review of risk management as part of our annual internal audit plan for 2021/22. The purpose of our review was to assess the policy and procedural aspects of risk management, along with the recording and reporting of risk, in light of the Service's move to the Business Management Information System (BMIS) to record its corporate risks in November 2021.

Risk management is undergoing a transitionary phase and the BMIS system represents a step change in:

- Accountability – in line with service values. Heads of service are now risk owners and will take more responsibility for updating their risk areas;
- Efficiency – including streamlining reporting;
- Clear audit trails – viewers can see current and historical updates clearly and provides a clear audit trail to assess adequacy and effectiveness of mitigating actions;
- Linkages – policy framework and project updates will be integrated into BMIS. As a result, the impact of risk updates on other areas of the business will be possible;
- Live updates – information will be available in real time. Risk owners are assigned to each issue with active mitigation in place;
- Integration – several other risk registers are being linked and referenced as control measures.

As part of this review we also conducted a risk management survey. The chart below represents the responses of 45 individuals at the Service to our risk management culture survey. 19 of the respondents described themselves as risk owners. We found that responses were broadly positive, supporting the view that the Service’s approach to risk management is evolving and progressing appropriately.


There is a consistent tone for risk management set from the top.
The organisation provides consistent, coherent, sustained and visible leadership in terms of how the it expects people to behave and respond when dealing with risk.
The organisation has clear leadership in terms of risk management.
Roles and responsibilities for managing risks have been well defined.
Risk management is well embedded in the organisation.
Individuals can talk openly about risks, without fear of consequences or being ignored.
Significant risks are identified and brought to the attention of Senior Management.
I have had sufficient training with respect to my responsibilities for risk management.
Risks are promptly de-escalated when controls have been applied.
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%
Strongly Agree
Agree
Don't know
Disagree
Strongly Disagree

Conclusion

We noted that there had been good progress made so far, with the organisation's move to BMIS for risk management, however, as part of the move from a framework supported by MS Word documents to the embedding of BMIS, our audit identified that some elements of the risk management control framework have not formally been in place throughout the transition and implementation, or are now in need of review and update to ensure that the risk management framework is effectively embedded and consistently applied.

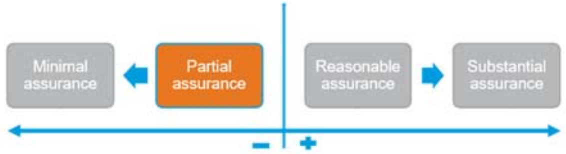
Our Risk Management survey of staff, including risk owners, found that the perception of risk management within the organisation was generally positive, further details can be found above.

Areas for improvement included ensuring that the draft Corporate Risk Management Policy is approved along with further supplementary guidance being established, a formal programme of training is developed and delivered and the Corporate Risks within BMIS are reviewed to ensure that the requirements of the risk management approach are consistently applied. We also noted that risk owner monthly reviews are not yet consistently taking place, operational risk registers at station level have not yet been developed and the organisation's risk appetite has not been reviewed since 2020. Whilst the Service is largely aware of the journey they are currently on and improvements required and are working towards these, it is important that these improvements are implemented to increase the effectiveness of the management of risk in the organisation.

Internal audit opinion:

Taking account of the issues identified, the Authority can take partial assurance that the controls upon which the organisation relies to manage this area are suitably designed, consistently applied or effective.

Action is needed to strengthen the control framework to manage the identified area(s).



Key findings

We identified the following findings:

Policies and procedures

Review of the draft Corporate Risk Management Policy found that it detailed how corporate risks are derived, the aims of risk management, the corporate risks themselves and high-level responsibilities. We noted that this policy was not yet in use and had not been formally signed off by the Chief Fire Officer. Additionally, we noted that the organisation’s risk appetite had not been reviewed since 2020 and was not documented within the Policy. We also found that there was no guidance in place on the arrangements for risk assessment, frequency of risk review by risk owners and the monitoring and reporting of risk through the governance framework. We were advised that this was currently being developed. There is a greater chance of risks not being managed effectively if an approved policy and supporting guidance is not in place. **(Medium)**

Training

We noted that a formal risk management training programme has not yet been developed to ensure that all staff groups have received and continue to receive the required training. This finding is supported by the results of our survey, where 25 of the 45 respondents answered "Don't Know" or "Disagree" to the statement "I have had sufficient training with respect to my responsibilities for risk management". There is a greater chance of risk being managed ineffectively if sufficient training is not delivered. **(Medium)**

Risk registers

We selected a sample of five Corporate Risks held in the BMIS system and noted that whilst risk descriptions detailed the cause of the risk, the impact of the risk was not clearly articulated. We also found that for one risk, relating to COVID, controls and future actions were not documented within BMIS. Whilst we appreciate that there is a separate process in place relating to the management of COVID, there is a greater chance of risks materialising if controls are not documented in BMIS and managed within the organisation's corporate risk framework. We also found that of the 22 open actions to mitigate risks in our sample of risks, 18 were overdue at the time of review. Additionally, we noted that the organisation is not currently recording the sources of assurance for individual risks. Where the Corporate Risk Management Framework is not consistently applied, there is a greater chance of risks materialising. **(Medium)**

Operational Risk Registers

We noted that operational risk registers, covering functional areas under CMT members were currently not in place and were due to be developed. In the absence of these operational risk registers, there is a greater chance of risks materialising at an operational level, which could potentially have wider organisational impact. **(Medium)**

Risk Owner Reviews

We were advised that, whilst monthly review of risks by risk owners was part of the revised approach to risk management in the organisation, these reviews had not yet commenced. There is a greater chance of risks materialising if they are not regularly reviewed and updated by risk owners. **(Medium)**

We noted the following controls to be adequately designed and operating effectively:

Identification of risks

We confirmed through review of a summary report presented at the Corporate Management Team Away Day in August 2021 that a Horizon Scanning Event was held in July 2021 where key risks had been identified. We were advised that these had been reviewed and incorporated, where appropriate, into the latest iteration of the organisation's corporate risks.

Linking Risks to Objectives

We selected a sample of five risks and confirmed that each had been linked to organisational objectives within the BMIS system.

Project and Programme Risks

We noted that programme and project risks were documented as part of programme and project raid logs. We selected a sample of three projects/programmes and confirmed that they followed a consistent format. Whilst there was less detail than for those risks deemed as Corporate in BMIS, this appears reasonable for the operational nature of the risks.

Risk Reporting

We reviewed Audit and Standards Committee meeting minutes and papers for September and December 2021 and confirmed that a CRR report was presented at each meeting. We noted that the reports provided Members with updates on risks and the minutes recorded discussion of the reports. We were advised that the full CRR was also due to be presented to the ASC going forwards.

We reviewed CMT agendas for December 2021 and February 2022 and confirmed that a Corporate Risk Register featured in each instance. We were advised that the CMT reviews the update prior to presentation of the updates to the Audit and Standards Committee.

2. DETAILED FINDINGS AND ACTIONS

This report has been prepared by exception. Therefore, we have included in this section, only those areas of weakness in control or examples of lapses in control identified from our testing and not the outcome of all internal audit testing undertaken.

1. Policies and procedures				
Control	There is a Corporate Risk Management Service Order in place which outlines some key elements of risk management. This document was issued in 2012 and has not been formally reviewed since this date. All non-critical service orders have been put on hold due to the COVID-19 Pandemic. A new Corporate Risk Management Policy is set to supersede the previous version as part of an organisation-wide exercise to rationalise and streamline the number of policies and service orders in place. A draft version has been developed which details how Corporate Risks are identified, the aims of risk management, the corporate risks themselves and high-level responsibilities but this document has not yet been formally signed off by the Chief Fire Officer and put into operation.		**Assessment:** **Design** **Compliance**	 × N/A
Findings / Implications	We noted that the Corporate Risk Service Order was currently on hold and had not been reviewed since 2012. Review of the draft Corporate Risk Management Policy found that it detailed how corporate risks are derived, the aims of risk management, the corporate risks themselves and high-level responsibilities. We noted that this policy was not yet in use and had not been formally signed off by the Chief Fire Officer. We also found that there was no guidance in place on the arrangements for risk assessment, frequency of risk review by risk owners and the monitoring and reporting of risk through the governance framework. We were advised that this was currently being developed. There is a greater chance of risks not being managed effectively if an approved policy and supporting guidance is not in place. We have also identified that the risk appetite is not documented in the Policy and has not recently been reviewed in section 6 of this report. We have addressed these issues in the management action for this section.			
Management Action 1	The draft Corporate Risk Policy will be approved and made available to relevant staff. Further guidance on risk assessment, review, monitoring and reporting will be established. The organisation's risk appetite will be formally documented in the Corporate Risk Policy and be subject to regular review for appropriateness.	**Responsible Owner:** Steve Frank, Head of Strategic Support and Assurance	**Date:** 31 July 2022	**Priority:** Medium

2. Training

Control	A formal risk management training programme has not been developed to ensure that all staff groups have received and continue to receive the required training.		**Assessment:**	
			Design	×
			Compliance	N/A
Findings / Implications	We noted that a formal risk management training programme has not yet been developed to ensure that all staff and officer groups have received and continue to receive the required training. This finding is supported by the results of our survey, where 25 of the 45 respondents answered "Don't Know" or "Disagree" to the statement "I have had sufficient training with respect to my responsibilities for risk management.". There is a greater chance of risk being managed ineffectively if sufficient training is not delivered.			
Management Action 2	A formal training programme for risk management will be developed and delivered, including refresher training at appropriate intervals.	**Responsible Owner:** Steve Frank, Head of Strategic Support and Assurance	**Date:** 31 December 2022	**Priority:** Medium

3. Corporate Risk Register - Risks

Control

The organisation's Corporate Risk Register is held in the BMIS system. For each Corporate Risk, the following is documented:

- risk description
- risk score
- controls

Assessances have not been documented for Corporate Risks.

Assessment:

Design	×
Compliance	N/A

Findings / Implications

We selected a sample of five corporate risks held in BMIS and found that:

- Whilst risk descriptions had been documented to articulate the cause of the risk, the impact of the risk was not clearly documented. There is a greater chance of risks being misinterpreted if the cause and effect of each risk is not clearly documented.
- Each risk had a risk owner documented
- Each risk had an inherent and current risk score documented
- Four of the five risks had controls documented, with Risk 9 (COVID risk) having no associated controls documented. Whilst we appreciate that there is a separate dedicated process in place relating to the management of COVID, there is a greater chance of risks materialising if controls are not documented in BMIS and managed within the organisation's corporate risk framework.
- Of the four risks with documented controls, we noted that controls were well worded, referring to control activities.
- We also noted that the organisation is not currently recording the sources of assurance for individual risks. There is a greater chance of risks materialising if assurances are not documented and considered when risks are reviewed.

We have also identified issues with actions allocated to risks within the next section and have addressed this issue in the management action for this section.

Management Action 3

We will develop the CRR held within BMIS to ensure:

- Risk descriptions clearly describe both the cause and impact of a risk
- All risks have controls documented against them
- Sources of assurance are recorded against each risk
- All risks have future actions documented
- All future actions are reviewed and updated if the due date is reached.

Responsible Owner:	Date:	Priority:
Steve Frank, Head of Strategic Support and Assurance	31 March 2023	Medium

4. Corporate Risk Register - Actions

Control	Where further action is required to reduce a Corporate Risk's risk score, actions will be documented within BMIS, assigned an action owner and a timeframe for completion.	**Assessment:** **Design** ✓ **Compliance** ×
Findings / Implications	We confirmed for our sample of five risks from the CRR in BMIS that: • Four of the five risks had future actions documented. Risk 9 did not have future actions documented. • For the four risks with actions documented, each action had been assigned a timeframe for completion and action owner. • We also noted that 18 of the 22 open actions in our sample were overdue. The majority of these overdue actions had due dates of 31/03/22 and the information for this sample was received in April 2022. There is a greater chance of risks materialising if all risks do not have actions with responsible owners whose timeframes are reviewed and updated as they are reached. We have agreed an action in finding three for this issue.	
Management Action	Please see finding three above.	

5. Functional Risks

Control	Functional (operational) risk registers have not been developed. In the absence of full operational risk registers, there is no process for the escalation of risks from operational registers to the corporate risk register.		**Assessment:** **Design** × **Compliance** N/A	
Findings / Implications	We noted that operational risk registers, covering functional areas under CMT members were currently not in place and were due to be developed. In the absence of these operational risk registers, there is a greater chance of risks materialising at an operational level, which could potentially have wider organisational impact.			
Management Action 4	We will develop functional risk registers and an escalation process for escalating operational risks to the Corporate Risk Register. We will also develop a process for the regular review of functional risks by an appropriate group/committee.	**Responsible Owner:** Steve Frank, Head of Strategic Support and Assurance	**Date:** 31 March 2023	**Priority:** Medium

6. Risk Appetite				
Control	The risk appetite of the organisation was agreed by Authority members in 2020 but has not been revisited since then to confirm that it is still accurate.		**Assessment:** **Design** **Compliance**	 × N/A
Findings / Implications	We reviewed the organisation's current risk appetite, documented within a paper presented to the Audit and Standards Committee in December 2021. We were advised that the organisation's risk appetite had not been reviewed since 2020 when it was agreed. We also noted that one respondent to our survey stated that the risk appetite was far too low for the organisation. There is a greater chance of risks impacting the achievement of organisational objectives if the risk appetite is not regularly reviewed for appropriateness. Review of meeting minutes for the January 2020 CMT meeting found that there was some evidence of overarching review of the risk register. We were, however, not provided with meeting minutes to evidence the previous six-monthly review of risks by CMT. There is a risk of the Service being unable to demonstrate scrutiny and challenge of its risk management if a clear record of this is not maintained.			
Management Action	Please see Management Action agreed in section one.			

7. Risk Owner Reviews				
Control	Corporate Risks have been assigned a frequency of monthly for review by risk owners. These reviews are yet to begin taking place.		**Assessment:** **Design** **Compliance**	 × N/A
Findings / Implications	We were advised that, whilst monthly review of risks by risk owners was part of the revised approach to risk management in the organisation, these reviews had not yet commenced. There is a greater chance of risks materialising if they are not regularly reviewed and updated by risk owners.			
Management Action 5	Risk owners will review their assigned risks on a monthly basis and ensure updates are recorded within BMIS.	**Responsible Owner:** Steve Frank, Head of Strategic Support and Assurance	**Date:** 31 July 2022	**Priority:** Medium

EXECUTIVE SUMMARY – HUMAN RESOURCES – GREY BOOK RECRUITMENT

Why we completed this audit

The objective of the audit was to assess the control framework in place regarding the Human Resources Grey Book Recruitment Campaign. The 'Grey Book' or the scheme of conditions of service of the National Joint Council for Local Authority Fire and Rescue Services being wholetime and retained duty staff and also control room uniformed staff, our testing included wholetime and retained duty staff. This included a review of the methods introduced by the Authority to advertise vacancies, the transparency of the recruitment process, and how equality is achieved throughout this process.

Annually, the Authority recruits firefighters including appointing those with On-Call experience to wholetime positions in line with the allocated recruitment budget. Following the global impact of COVID-19, the Authority adapted the annual campaign approach to ensure the recruitment for wholetime positions could continue. This was achieved via additional practical assessment centres but with fewer attendees to ensure social distancing, virtual interviews, and the introduction of an App which scans individuals and issues body measurements to the Stores Department to avoid frequent physical contact when fitting BedsFRS uniform.   A safe system of work (SSOW) was put in place to allow for the measuring of personal protective clothing (PPE) and Breathing Apparatus (BA).

The Authority launched a campaign in May 2021 with the intention of new recruits commencing employment from February 2022. To support the campaign and to ensure diversity and equality in the methods of entry, the Authority utilised targeted social media advertising to ensure they were targeting key demographics within the local communities. We found a total of 332 individuals submitted an application for the role of Firefighter as a result of advertisments via social media campaigns and ‘Have a Go Days’. We found that of the 332 applicants that had applied, 192 (58 per cent) were progressed to online testing which we noted were completed in a timely manner. Of the 192 progressed, 101 (53 per cent) were progressed to practical assessments. Furthermore, we noted that of the 101 candidates, 40 successfully passed the online assessments, practical assessments and interviews with 14 appointed into fulltime roles and 26 placed on a holding list. These 26 staff have passed the initial recruitment stages (online testing, interviews, presentation) and were placed onto a holding list to be selected when the Authority needs to employ additional staff, this approach is considered to be more efficient.

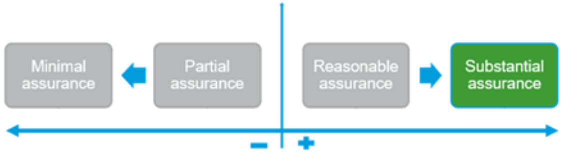
We noted the target of 40 successful applicants was achieved by February 2022 as forecasted within the January 2022 Corporate Management Team (CMT) Report.

Conclusion

Our review found that the Authority had in place an On-Call Recruitment Policy and Procedure to support the recruitment of firefighters for the 2021/22 Grey Book Campaign. As part of the process, the initial applications and testing were anonymised to avoid any bias, with this further supported by fixed questions and a clear scoring methodology once applicants progressed to interview to ensure consistency and clarity in how the final scores were obtained. There is also a clear policy in respect of applying reasonable adjustments where required. Through review of a sample of 20 candidates, we confirmed the Authority was compliant with the Policy and found candidates were filtered out of the recruitment process via online tests, assessment centres, and interviews conducted by three panellists. Furthermore, we found pre-employment vetting checks were performed against successful candidates and noted formal signed contracts were retained electronically by the Authority. We confirmed the Service's overall recruitment campaign was effectively executed as we noted the quota identified in January 2020 by the CMT of 40 individuals were successfully filled by the February 2022 target. We noted this comprised of 14 individuals appointed into wholetime roles and 26 placed on a holding list.

Internal audit opinion:

Taking account of the issues identified, the Authority can take substantial assurance that the controls upon which the organisation relies to manage this area are suitably designed, consistently applied and effective.



Key findings

We identified the following findings:

We noted the following controls to be adequately designed and operating effectively:

On-Call Recruitment Policy

The Authority has developed an On-Call Recruitment Policy and Procedure which supports the recruitment of grey book campaign staff. The Policy details key guidance on the recruitment process of new employees, and record keeping. We confirmed the Policy was accessible by staff via Sharepoint and were informed by the Resourcing Manager that the Policy was made available to Human Resources staff during initial inductions.

Grey Book Recruitment Methodology

We obtained a January 2020 Corporate Management Team (CMT) Report and confirmed it detailed the Authority's Grey Book Campaign approach. As per the report, we noted the Authority intended on launching a 2021/22 recruitment campaign initiating in April/ May 2021 and ending in May 2022 to meet operational demands. To support this, we were advised by the Resourcing Manager that annually, the Authority's overall budget is reviewed, and additional allocations are made for the recruitment of firefighters. Through review of correspondences between the Head of Human Resources and the Assistant Chief Fire Officer, we confirmed the recruitment approach for 40 candidates in respect of budget requirements was agreed at a senior management level. This was further corroborated through review of the February 2020 Fire and Rescue Authority (FRA) meeting minutes. As at April 2022, we confirmed the Service had effectively met the resourcing requirements of 40 candidates as we found 14 individuals were appointed into fulltime roles and 26 were placed onto a holding list.

Selecting the Strongest Candidates

The Authority utilises various social media channels to broadcast vacancies to the public. Furthermore, we found the public and potential candidates were capable of recording their interest in vacancies via an online register. We were advised by the Recruitment Manager that the use of the register your interest enabled the Authority to carryout Positive Action initiatives targeting the Authority's underrepresented groups.

Furthermore, we found that of the 332 applicants that had completed an application, 192 (58 per cent) were progressed to online testing in a timely manner. Of the 192 progressed, 101 (53 per cent) were progressed to practical assessments in a timely manner.

Online Testing

We obtained an April 2021 to March 2022 Report of Candidates to be considered to fill the Authority's Grey Book Campaign vacancies. We selected a sample of 20 candidates which consisted of wholetime and retained on-call staff. We confirmed in all instances, online test invitations were issued to individuals by email via the OLEEO recruitment system. We confirmed in all instances, tests were completed by candidates and noted test results were recorded within the testing portal in a timely manner. Of the 20 samples reviewed, we found in 15 instances candidates scored greater than 60 per cent in both the verbal reasoning and calculation tests. We therefore confirmed the 15 candidates were progressed to the practical assessments and noted confirmation emails were issued to the individuals via OLEEO. In the remaining five cases, we noted candidates scored below 60 per cent in either both or one of the tests and as such were not progressed.

Interview Invitations

Using the same sample of 20 candidates selected above, we confirmed that 15 individuals successfully passed the Authority's online tests. We found in all 15 instances, candidates were issued with automated standardised invitations for practical assessments. Of the 15 individuals that were invited to practical assessments, 13 were successful. Additionally, we found all 13 individuals were offered formal interviews and found they were captured within an overall ranking spreadsheet. We noted the spreadsheet captured both the online and practical test scores in addition to the presentation and interview scores.

Interviews Conducted

Using the same sample of 20 candidates, we found interviews were conducted in 13 instances for those that successfully passed online assessments and the practical assessments. We confirmed the interview panels consisted of one Human Resources representative and two Operational Personnel. We found in all 13 instances, outcomes of interviews were clearly recorded within the Authority's OLEEO HR system. We noted 11 of the 13 candidates were successful and noted in all instances, outcomes were communicated via automated emails from OLEEO.

✓ Employment Checks

From the sample of 20 candidates,11 were successful and therefore required pre-employment vetting. We confirmed the Authority performed pre-employment vetting checks against 11 successful candidates with core documents reviewed which included passports, medical including fitness tests, employment references, and outcomes of Disclosure and Barring Service (DBS) checks via a third-party (Due Diligence Checking Ltd).

✓ Position Acceptance

Of the 11 successful candidates, we confirmed positions were accepted in ten instances. We noted formal contracts were signed by candidates and retained electronically by the Authority. In the remaining instance, we noted a candidate failed a pre-employment vetting check and consequently, a formal contract was not issued to the individual.

✓ Lessons Learnt

Through discussion with the Resourcing Manager, we were informed that various measures were put in place to adapt to the changing environment presented by COVID-19. These included the use of remote interviews and virtual etiquette guidance documents, a reduction in the number of candidates attending practical tests, and the introduction of a uniform sizing app. By adapting the interview process, we were informed by the Recruitment Manager that the Service identified greater efficiency and flexibility resulting in an increased panellist turnout. Similarly, we were advised by the Resourcing Manager that the introduction of the app had greatly improved the efficiency of the service as virtual size fittings for new starters could be taken without the need to visit in person. Going forward, it is anticipated that both the app and use of remote interviews where appropriate will continue to be used by the Service to ensure that the efficiencies identified are transferred into the post-COVID work environment.

For more information contact

Name: Suznne Rowlett, Head of Internal Audit

Email address: suzanne.rowlett@rsmuk.com

Telephone number: 07720 508148

Name: Louise Davies, Manager

Email address: louise.davies@rsmuk.com

Telephone number: 07720 508146

rsmuk.com

The matters raised in this report are only those which came to our attention during the course of our review and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. Actions for improvements should be assessed by you for their full impact. This report, or our work, should not be taken as a substitute for management's responsibilities for the application of sound commercial practices. We emphasise that the responsibility for a sound system of internal controls rests with management and our work should not be relied upon to identify all strengths and weaknesses that may exist. Neither should our work be relied upon to identify all circumstances of fraud and irregularity should there be any.

Our report is prepared solely for the confidential use of Bedfordshire Fire and Rescue Authority and solely for the purposes set out herein. This report should not therefore be regarded as suitable to be used or relied on by any other party wishing to acquire any rights from RSM UK Risk Assurance Services LLP for any purpose or in any context. Any third party which obtains access to this report or a copy and chooses to rely on it (or any part of it) will do so at its own risk. To the fullest extent permitted by law, RSM UK Risk Assurance Services LLP will accept no responsibility or liability in respect of this report to any other party and shall not be liable for any loss, damage or expense of whatsoever nature which is caused by any person's reliance on representations in this report.

This report is released to you on the basis that it shall not be copied, referred to or disclosed, in whole or in part (save as otherwise permitted by agreed written terms), without our prior written consent.