Cambridgeshire and Peterborough Fire Authority

Internal Audit Progress Report

19 January 2023

RSM

Contents

1 Key messages

This report below provides a summary update on progress against each plan and summarises the results of our work to date. The reports finalised since the last Committee are highlighted in **bold** below.

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

Assignment	Status	Actions agreed			Opinion Issued
		L	M	H	
Risk Management	Final	1	0	0	Substantial Assurance
Debrief Following Complex Incidents	Final	0	2	0	Reasonable Assurance
General Data Protection Regulation (GDPR) Governance	**Final**	**7**	**8**	**1**	**N/A - Advisory**
Key Financial Controls – General Ledger and Budgetary Control	**Final**	**0**	**1**	**0**	**Reasonable Assurance**
System Ownership Governance	In Progress				
Integrated Risk Management Planning Framework	In Progress				
Governance	In Progress				
ICCS and Mobilising System	To commence 3 March 2023				
Follow Up	To commence 21 March 2023				

Appendix A – Other matters

Annual Opinion 2022/23

The Overview and Scrutiny 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.

Changes to the audit plan

Since the last Overview and Scrutiny Committee, we have postponed the review of ICCS and Mobilising System due staff absence within RSM. This is now due to commence on 3 March 2023.

Information and briefings

Since the last Overview and Scrutiny Committee we have issued our Quarterly Emergency Services client briefing.

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 B – Executive summaries and action plans (High and Medium only) from finalised reports

EXECUTIVE SUMMARY – GENERAL DATA PROTECTION REGULATION (GDPR) GOVERNANCE

Why we completed this audit

From 25 May 2018 the General Data Protection Regulations (GDPR) replaced the EU Directive 95/46/EC. The UK Data Protection Act (DPA) 2018 was introduced at the same date to provide the legislative basis for GDPR in the UK.

Whilst many of the GDPR/DPA 2018 main concepts and principles remain largely the same as those in the previous UK DPA, there are significant new elements and enhancements which will require companies and organisations to perform some specific compliance activities for the first time. In particular, GDPR places greater emphasis on the documentation that data controllers must keep to demonstrate their accountability.

We have been commissioned to perform an Agreed Upon Procedures (AUP) assignment of the current data governance processes, procedures and controls. The scope of this GDPR audit includes a broad range of coverage given the remit of GDPR and the corresponding UK DPA Act 2018. Moreover, this assignment is designed to assess the current control framework in place and to evaluate opportunities for future areas of controls development, based on the evidence presented to us. This takes into account both ICO guidance and relevant best practice identified at other similar organisations, providing a high-level framework of actions, where applicable.

Our report is a factual report and we do not provide a level of assurance, or internal audit opinion, and should not be taken to provide such.

Headline findings

All management actions have been prioritised below to inform internal planning, of which there are one high, eight medium and seven low priority actions.

The key findings from this review are as follows:

Data Flow Mapping

Through review of the Record of Processing Activities (RoPA) for the processing where the Service is the Controller, we noted that the categories of recipients or the data owner were not being recorded. We also noted that the RoPA for COVID-19 related information was not in a consistent format with the Controller RoPA, for instance, it did not cover GDPR Article 6 lawful basis for processing.

Furthermore, we noted blank fields in the RoPAs, such as the Purpose of Processing (one missing entry), Link to Data Protection Impact Assessment (two missing entries) and Data Protection Act 2018 Schedule Condition for processing (one missing entry) in the Controller RoPA and the 'Names of third countries or international organisations that personal data are transferred to' and 'Safeguards for exceptional transfers of personal data to third countries or international organisations' for one entry in the Processor RoPA. If data is not appropriately mapped across the organisation, there is a risk of the organisation being unaware of the data being held, how such data is used by different departments and how it flows through the organisation. This could also lead to issues with lawfulness of processing, security and retention. (**Medium**)

Third Parties

We were advised by the Information Governance Manager that a central register of all third parties whom personal data is transferred to, is not maintained. Instead, third parties are identified as part of the RoPA process. Through review of the RoPA, we noted that whilst it recorded whether data transfer arrangements were in place, further information was not provided, such as the start and end date of the agreements where relevant. This can lead to ineffective tracking of third parties, resulting in personal data being shared without appropriate safeguards. (**Medium**)

We confirmed through review that a standard set of Terms & Conditions of Contract had been produced which is used as part of agreements and had a section on Data Protection Act 2018, covering the processing of personal data. We however found several areas not included, such as the categories of data subject or the fact that the processor must give the controller whatever information it needs to ensure they are both meeting their Article 28 obligations. This can result in personal data being shared with third parties without appropriate safeguards. (**Medium**)

Data Storage and Retention

Through review of the Information Retention Policy, we noted certain information not covered, such as preserving physical records (storage conditions etc.). We also noted that whilst a retention schedule was encompassed in the policy, some areas were not detailed, such as the record owner. Furthermore, we noted that the schedule was not fully completed, for instance, the method of disposal was not being consistently recorded. Without a comprehensive policy and schedule in place, this can lead to an inconsistent approach to data storage and retention, potentially leading to personal data being mismanaged. (**Medium**)

Training

We obtained reports of Information Governance training compliance as at September 2022 and found that there were 475 course completions out of 1294 in the last 12 months (covering both the Data Protection and Information Security training (36.7%) and 236 out of the 647 staff were certified i.e. had passed the test at the end of the course (36.5%)). The Information Governance Manager however advised that there was no formal process for escalating non-compliance with training. This can lead to staff not being kept up to date with data protection practices and requirements, increasing the risk of a data breach as a result of user error. (**High**)

Personal Data Requests

Through review of the Subject Access Request (SAR) Log, we noted that whilst it recorded requests received from data subjects, it did not cover some areas such as whether the request has been made by a third party on behalf of a data subject. We also noted that it was not fully completed, for instance, the date due column was blank for 18 of the 21 entries. This can lead to key information in respect of personal data requests not being retained for analysis and investigation where required, resulting in process improvements not being identified or issues not being resolved appropriately. (**Medium**)

Lawful Bases (including Consent)

Through discussion with the Information Governance Manager, we were advised that although the organisation is aware of the lawful bases it uses to process personal information (such as consent), this had not been formally and centrally documented and agreed. If the lawful bases identified by the organisation are not documented, there is a risk that staff will be unaware of the lawful bases in which personal data is obtained, or lawful bases being inconsistently applied. This can lead to a lack of understanding by staff with respect to lawful bases used for personal data obtained should a query arise. (**Medium**)

On review of template consent forms (Workplace Adjustment Passport, Photograph Consent Form – Adult, Photograph Consent Form – Children, and Stay Safe in the Home), we found that whilst all forms sought explicit consent, they did not cover consistent areas, for instance, the Workplace Adjustment Passport did not reference a privacy notice, whereas other forms did. This can lead to the organisation not informing data subjects of key information prior to obtaining their consent to process their personal data. (**Medium**)

Data Breaches

Through review of the DPA Data Breach Log, we noted that whilst details of breaches were being recorded, some information was not being covered, such as the format of the data lost/impacted. This can lead to key data breach information not being retained to ensure sufficient audit trail in the event of a data breach investigation by the ICO and to inform thematic analysis of breaches to identify trends to be addressed. In partial mitigation, we noted that some information was being recorded on the Data Breach Reporting Form, such as whether sensitive personal data was compromised. (**Medium**)

We also made the following observations which did not result in a management action being agreed:

GDPR Action Plan

Through review of the GDPR Action Plan, we noted that all actions had been marked as complete. Through review of the Information Governance & Security Management Report for September 2022, we confirmed that an update had been provided on the Action Plan, noting it as complete. We were advised by the Information Governance Manager that the September 2022 meeting minutes were not yet available at the time of the audit, however, we were provided with an agenda for the meeting which included 'Sign off of GDPR Action Plan'.

Data Protection Procedure

Through review of the Data Protection Procedure, we noted that it had been last updated in January 2022 with a next review date of January 2023. We also confirmed via a screenshot that the Procedure had been made available to staff on the intranet. In terms of content, we noted that the Procedure covered key areas such as GDPR principles, lawful bases and rights under GDPR.

Data Protection Officer

Through review of the Job Description of the Information Governance Manager, we confirmed that they had the responsibility to act as the Authority's data protection officer (DPO), ensuring the Authority is fully compliant with its data protection obligations under the General Data Protection Regulations (GDPR), following best practice, advising senior managers, improving processes and completing audits and reviews.

We also noted that they reported to the Head of Media, Communication and Transparency, who sits on the Strategic Board and Chief Officers Advisory Group, and had a dotted line to the Deputy Chief Executive Officer in practice, as advised by the DPO. We confirmed that the DPO held a EU GDPR Practitioner qualification from the International Board for IT Governance Qualifications.

Finally, we were provided with written confirmation of the following: 'As per the UK GDPR the Information Governance Manager for Cambridgeshire Fire & Rescue Service operates independently. They do not determine the purposes and means of the processing of personal data within the organisation or have decision making responsibilities which may cause a conflict of interest. Advice and guidance is provided to employees of Cambridgeshire Fire & Rescue Service to ensure the Service is lawfully compliant. The Information Governance Manager does not receive any instructions regarding the exercise of their tasks.'

DETAILED FINDINGS AND ACTIONS

This report has been prepared by exception.

Data Flow Mapping				
Control	A Record of Processing Activities (RoPA) template has been produced which covers areas such as: • purpose of the processing; • categories of individuals; • GDPR Article 6 lawful basis for processing; and • where the data is stored.			
Findings / Implications	Through review of the RoPA for the processing where the Service is the Controller, we noted that the categories of recipients or the data owner was not being recorded. We confirmed that the RoPA for where the Service is the Processor covered the required areas under GDPR. We however noted that the RoPA for COVID-19 related information was not in a consistent format with the Controller RoPA, for instance, it did not cover GDPR Article 6 lawful basis for processing. We also noted blank fields in the RoPAs, such as the Purpose of Processing (one missing entry), Link to Data Protection Impact Assessment (two missing entries) and Data Protection Act 2018 Schedule Condition for processing (one missing entry) in the Controller RoPA, and the 'Names of third countries or international organisations that personal data are transferred to' and 'Safeguards for exceptional transfers of personal data to third countries or international organisations' for one entry in the Processor RoPA. If data is not appropriately mapped across the organisation, there is a risk of the organisation being unaware of the data being held, how such data is used by different departments and how it flows through the organisation. This could also lead to issues with lawfulness of processing, security and retention.			
Management Action 1	The Record of Processing Activities (RoPA) for where the Service is the Controller will be updated to include the categories of recipients and the data owner. Following this, the Service will ensure that all RoPAs are fully completed and that a consistent format is used (for instance, COVID-19 related processing activities).	**Responsible Owner:** Danielle Wilkinson – Information Governance Manager (DPO)	**Date:** 30 April 2024	**Priority:** Medium

Third Parties				
Control	Third parties are tracked using the RoPA and a register of Information Sharing Agreements is also retained. A contract template is in place which has a section on the Data Protection Act 2018, which includes data protection related terms and clauses.			
Findings / Implications A	We were advised by the Information Governance Manager that a central register of all third parties whom personal data is transferred to, is not maintained. Instead, third parties are identified as part of the RoPA process. Through review of the RoPA, we noted that whilst it recorded whether data transfer arrangements were in place, further information was not provided, such as the start and end date of the agreements where relevant. This can lead to ineffective tracking of third parties, resulting in personal data being shared without appropriate safeguards. In partial mitigation, we noted that a register of Information Sharing Agreements was in place, however, this does not cover all third parties.			
Findings / Implications B	We confirmed through review that a standard set of Terms & Conditions of Contract had been produced which is used as part of agreements and had a section on the Data Protection Act 2018, covering the processing of personal data. We however found several areas not included, such as the categories of data subject or the fact that the processor must give the controller whatever information it needs to ensure they are both meeting their Article 28 obligations. This can result in personal data being shared with third parties without appropriate safeguards.			
Management Action 2a	A register of third parties to whom 'in scope' (personal) data is transferred to will be produced. For each third party, the organisation will record: • name of the third party; • whether there will be sharing of personal data with the third party (if it is a general register for all third parties/contracts etc.); • if the third party is a controller or processor; • whether a formal contract or other legal act is in place (this is a must for processors); • contract owner; • whether the contract contains the required contractual data confidentiality terms and conditions / clauses; • start and end dates of the contract; and • other contractual protections that have been put in place/assessed (especially where a contract is not in place), such as reviewing the third party's terms and conditions or privacy notices, or the use of a signed data/information sharing agreement.	**Responsible Owner:** Danielle Wilkinson – Information Governance Manager (DPO)	**Date:** 30 April 2024	**Priority:** Medium

Management Action 2b	The standard Terms & Conditions of Contract will be updated to cover the following with respect to the processing of personal data: • the subject matter of the processing; • the categories of data subject; • the controller's obligations and rights; • the processor must take appropriate measures to ensure the security of processing; • taking into account the nature of processing and the information available, the processor must assist the controller in meeting its UK GDPR obligations in relation to the security of processing; • the processor must delete existing personal data unless the law requires its storage; and • the processor must give the controller whatever information it needs to ensure they are both meeting their Article 28 obligations.	**Responsible Owner:** Danielle Wilkinson – Information Governance Manager (DPO)	**Date:** 30 April 2024	**Priority:** Medium

Data Storage and Retention				
Control	The Service has documented an Information Retention Policy which references areas such as: • roles and responsibilities; • legislative requirements; • physical archives; and • disposal. The Policy also includes a retention schedule as an appendix.			
Findings / Implications	Through review of the Information Retention Policy, we noted that it was next due for review in January 2023. We also reviewed a screenshot demonstrating that the Policy was available to staff on the intranet. In terms of content, however, we noted certain information not covered, such as preserving physical records (storage conditions etc.). We also noted that whilst a retention schedule was encompassed in the policy, some areas were not detailed, such as the record owner. Furthermore, we noted that the schedule was not fully completed, for instance, the method of disposal was not being consistently recorded. Without a comprehensive policy and schedule in place, this can lead to an inconsistent approach to data storage and retention, potentially leading to personal data being mismanaged.			
Management Action 4	The Information Retention Policy will be updated to cover: • managing the security of records; • preserving physical records (storage conditions etc.) • the ICO's advice that "personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes"; • how compliance is to be monitored (for instance, the policy should clarify the frequency and approach of audits); • record naming (naming conventions etc.); and • disciplinary information for breach of the policy. In addition, the retention schedule contained in the Policy will be updated to cover: • record owner; • retention trigger; and • action at the end of retention period (review for further retention, anonymise, destroy etc.). Following this, the Service will ensure that the schedule is fully completed.	**Responsible Owner:** Danielle Wilkinson – Information Governance Manager (DPO)	**Date:** 30 April 2024	**Priority:** Medium

Training				
Control	The Service has Information Governance training which has two areas that staff are required to complete as part of induction and annually thereafter: Data Protection and Information Security.			
Findings / Implications	Through review of screenshots of training content relating to the Information Governance training, we noted that this covered areas such as data protection and giving back control, subject information rights, recognising and reporting breaches, and email/internet use. We also confirmed that the Information Governance training had been included in the Induction Handbook. We however obtained reports of Information Governance training compliance as at September 2022 and found the following: • there were 475 course completions out of 1294 in the last 12 months (covering both the Data Protection and Information Security training (36.7%); and • 236 out of the 647 staff were certified i.e. had passed the test at the end of the course (36.5%). We were advised that overdue training is chased on an ad-hoc basis for high risk areas, with an example chaser email being provided from May 2022 and internal communications are circulated occasionally covering training, with an example provided covering data breaches and the importance of keeping up to date with training packages. The Information Governance Manager however advised that there was no formal process for escalating non-compliance with training and further formal action had not been undertaken to address training compliance. This can lead to staff not being kept up to date with data protection practices and requirements, increasing the risk of a data breach as a result of user error.			
Management Action 5	Firm action will be taken to ensure increased compliance with the Information Governance training. This will include a formal process for chasing overdue training and escalation of non-compliance.	**Responsible Owner:** Danielle Wilkinson – Information Governance Manager (DPO)	**Date:** 31 January 2023	**Priority:** High

Management Action 8b	The Subject Access Request (SAR) Log will be updated to cover: • date request logged; • who the request has been received from (ideally pseudonymised, or if using a form, the form reference); • date identity verified; • whether the request has been declined; • if declined, why the request has been declined; • if declined, when the data subject was informed of this; • whether the request has been made by a third party on behalf of a data subject; • if the request has been made by a third party, whether the authority of the third party has been established; • date authority established; • if the request has been made by a third party, whether the identity of the third party has been verified; • date third party identity verified; • in what format the information has been sent to the data subject; • whether there has been an extension to the deadline; • if there has been an extension, when the data subject was informed; and • whether the information was sent to the data subject within the required deadlines. Following this, the Service will ensure that the Log is fully completed.	**Responsible Owner:** Danielle Wilkinson – Information Governance Manager (DPO)	**Date:** 30 April 2024	**Priority:** Medium

Lawful Bases (including Consent)				
Control	The Service has not yet formally agreed and centrally documented its lawful basis for the different types of data it processes. A Consent Guidance document has been produced to help staff decide if consent is required to process personal data and if so how to capture and record that consent in a legal manner. Where consent is required, consent forms are in place for this.			
Findings / Implications A	Through discussion with the Information Governance Manager, we were advised that although the organisation is aware of the lawful bases it uses to process personal information (such as consent), this had not been formally and centrally documented and agreed. If the lawful bases identified by the organisation are not documented, there is a risk that staff will be unaware of the lawful bases in which personal data is obtained, or lawful bases being inconsistently applied / Lawful Bases (just no rationale): This can lead to a lack of understanding by staff with respect to lawful bases used for personal data obtained should a query arise.			
Findings / Implications B	Through review of the Consent Guidance, we noted that it was next due for review in January 2023. We also confirmed that the Guidance had been made available to staff on SharePoint. We noted that whilst the Guidance set out key considerations when obtaining consent, certain information was not covered, such as how to identify and verify the age of data subjects to ensure that parental consent is obtained where required. This can lead to the organisation not informing data subjects of key information prior to obtaining their consent to process their personal data.			
Findings / Implications C	We obtained the following consent forms: • Workplace Adjustment Passport; • Photograph Consent Form - Adult; • Photograph Consent Form - Children; and • Stay Safe in the Home. We noted through review that whilst all forms sought explicit consent, they did not cover consistent areas, for instance, the Workplace Adjustment Passport did not reference a privacy notice, whereas other forms did. This can lead to the organisation not informing data subjects of key information prior to obtaining their consent to process their personal data.			
Management Action 9a	The Service will formally document and agree the lawful bases for the different types of data processed by the organisation. This will include the rationale for the lawful bases as relevant. Subsequently, this will be communicated to relevant staff.	**Responsible Owner:** Danielle Wilkinson – Information Governance Manager (DPO)	**Date:** 30 April 2024	**Priority:** Medium
Management Action 9c	As part of the update to Consent Guidance, the following areas will be referenced for coverage in consent forms: • the name of the organisation/any third-party controllers who will rely on the consent;	**Responsible Owner:** Danielle Wilkinson – Information Governance Manager (DPO)	**Date:** 30 April 2024	**Priority:** Medium

	• a copy of the privacy notice or reference to this and where it is available; • why the organisation wants the data (the purposes of the processing); • what the organisation will do with the data (the processing activities); • whether the data will be shared with any other organisations; • the fact that data subjects can withdraw their consent at any time; and • a recording of explicit consent (rather than implied), including the date when consent was given. Following this, the Service will review existing consent forms and ensure all areas are covered.			

Management Action 10b	The Data Breach Log will be updated to cover: • date the breach was reported internally; • content of data lost/impacted; • whether sensitive personal data was lost/impacted; • format of data lost/impacted; • source of data lost/impacted; • the categories of those affected by the breach (employees, service users etc.); • consequences of the breach; • when the breach was notified to the ICO (where relevant); • whether the breach was notified to the ICO within 72 hours (where relevant); • when the breach was notified to the individuals (where relevant); • when the breach was notified to the relevant management forum; • actions taken/to be taken to guard against reoccurrence; and • date actions completed.	**Responsible Owner:** Danielle Wilkinson – Information Governance Manager (DPO)	**Date:** 30 April 2024	**Priority:** Medium

EXECUTIVE SUMMARY – KEY FINANCIAL CONTROLS – GENERAL LEDGER AND BUDGETARY CONTROL

Why we completed this audit

We have undertaken a Key Financial Controls review, specifically focussing on the areas of the General Ledger and Budgetary Control and Reporting as part of the 2022/23 approved Internal Audit Plan. The objective of the review was to allow the Authority to take assurance over the design and robustness of processes in place to manage these key financial control systems.

The Financial Regulations and Financial Control Standards document which set out the approach to control and management of key financial areas. Additionally, a Statement of Delegated Responsibilities is in place which outlines the delegated authority and financial approval limits of staff. The Dream finance system is utilised, access to which is controlled by different username and passwords, and access rights to the system are assigned based on job role. The Finance Team overseen by the Finance Manager, is responsible for managing the budgeting, accounting, and financial reporting activities.

A budget requirement of £31.2m for 2022/23 was approved by the Fire Authority in February 2022. Monthly budget statements are produced and bi-monthly meetings are held with budget holders to review the budget statements with significant variances identified and discussed. Monthly Budgetary Control Reports are also presented to the Deputy Chief Executive for oversight and scrutiny.

Conclusion

Overall, we confirmed through our review that the Authority has generally well-designed and consistently applied key financial controls to manage the General Ledger and Budgetary Control and Reporting areas. We identified through our review there are up to date financial governance documentation to control and manage these key financial areas. In addition, we also noted areas of effective control design and compliance regarding the Dream system access, Dream system backups, month-end timetable, and control reconciliations.

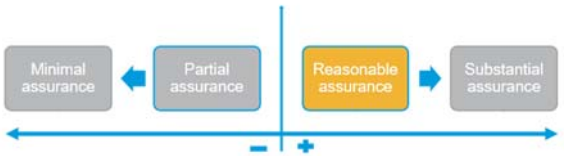
A Budget Book is produced which provides a comprehensive overview of the annual budget and is subject to review and approval by the Fire Authority. We also identified the monthly issue of Budgetary Control Reports (BCR) for review by the Deputy Chief Executive and that financial performance figures reported on the BCR aligned with figures on the Dream System. Additionally, we found that there is e-learning training material on how to use Dream, raise purchase orders, invoices, and budget monitoring processes for budget holders.

However, we noted issues in relation to independent month-end review of journals.

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 areas.



Key findings

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

Journals

Testing of a sample of 20 journals noted three instances in October 2022 where the Senior Financial Accountant prepared the journals and completed the month-end journal review thereby lacking a segregation of duties. If journals are not independently reviewed, there is a risk that transactions may not receive the appropriate scrutiny and challenge which may result in financial losses. **(Medium)**

We have identified the following areas as well-designed and effective:

General Ledger

Policies and Procedures

Review of the Financial Principles and Financial Control Standards confirmed they outlined the approach to control and management of key financial areas, including general ledger and budgetary control and reporting. Review of the Statement of Delegated Responsibilities confirmed it outlined the delegated authority and financial approval limits of staff, including the Chief Fire Officer and budget holders.

Review of the individual documents noted that they had been reviewed in line with the review frequency and were up to date. Review of a screenshot of the finance shared drive also confirmed the finance governance documents had been shared and made available to staff.

Dream Financial System Access

We obtained the user report with the list of all current users with access to the Dream Finance System as of 16 November 2022. We selected a sample of five active users and confirmed through review of ResourceLink that all users are still employed by the Authority. For a sample of five leavers, we confirmed through review of the Dream Finance System active users report that they have been removed from the system.

Dream Financial System Backup

We selected a sample of three days (13, 14, and 15 November 2022) and a review of screenshots of the drive confirmed completion of system backups. Review of the screenshots also noted that the Dream Finance system was backed up daily every four hours.

Month-End Timetable

The Authority has in place a month-end timetable, recorded within an Excel spreadsheet, that outlines key finance month-end activities, including Dream system closedown, journal review, and bank reconciliations.

Review of the month-end checklists for August, September, and October 2022 noted that each task was recorded as complete alongside the date and initials of individuals who completed the task. We also confirmed through review of the month-end checklists for August, September, and October 2022 that in all instances the checklists had been reviewed and signed by the Head of Finance or Senior Finance Accountant.

Control Account Reconciliations

We selected a sample of five control accounts B215 – Debtors, B379 - Project Suspense, B305 – Accruals, B300 - Purchase Ledger, and B240 Bad Debt Provision. Through review of the control account reconciliations for August, September, and October 2022 we confirmed that all reconciliations had been completed and reviewed in a timely manner. We also noted that in 14 out of 15 instances, no variances had been recorded. In the remaining instance in September 2022 the Purchase Ledger had a variance of £271.20, this was investigated and cleared.

Budgetary Control and Reporting

2022/23 Annual Budget

We confirmed through review of the 2022/23 Budget Book that the Authority set a budget requirement of £31.2m. Review of the Fire Authority February 2022 minutes noted the Authority discussed and approved the 2022/23 budget. Reconciliation of a sample of five figures from the finalised budget as approved by the Fire Authority in February 2022 to the budget uploaded onto Dream in the same month noted in all instances the figures matched.

Performance Reporting

Review of the August, September, and October 2022 Budgetary Control Reports (BCR) confirmed that the Deputy Chief Executive received these with updates on the Authority's financial performance for oversight and scrutiny. Review of the August, September and October 2022 BCR noted they outlined the budget to date and actual to date spend with necessary comments on significant under and overspends.

Budget Monitoring and Review

Budget Control Reports are prepared, and Budget Holder bi-monthly meetings are held with budget holders to review the budget statements with significant variances identified and discussed, with actions being agreed to address significant variances and followed up in subsequent meetings. Testing of a sample of three cost centres confirmed in all instances that budget control reports had been produced for budget holders for September and October 2022 highlighting original budget, virements, revised budget, actual to date and the variances.

We obtained the September budget holder meeting notes for the three cost centres and confirmed in all instances they included discussion on budget overspends and underspends. We also noted that reasons for the variances were identified within the meeting notes. We also noted through review of the ICT Shared Services and Health and Safety Services meeting notes that they included a 'Mid-Year Review' tab which detailed notes from mid-year financial review meetings held by the Finance Manager and budget holders.

Reconciliation of BCR figures to Dream Financial System

We selected a sample of three figures (Senior Management (Hay), Fire Equipment and Other Income) from the BCR presented for review and oversight to the Deputy Chief Executive in August, September, and October 2022 and reconciled the figures to the Dream system for the corresponding months. Testing confirmed in six instances, the figures on the BCR aligned with the figures on the Dream system. In the remaining three instances, we identified differences in the figure for fire equipment on the system and the figure reported in the BCR. We were advised by the Senior Financial Accountant that the difference is due to occupational health equipment repairs and maintenance classified as fire equipment repairs on the Dream System and as other supplies and services on the BCR.

Budget Holder Support and Training

We noted through walkthrough of Learning Pool that budget holders have access to learning resources relating to raising purchase orders, invoices, and budget reports. We also noted that budget holders had to complete a quiz to test understanding of the training. We sought to obtain training logs to confirm overall completion of training provided to budget holders, however, were informed by the Senior Financial Accountant that no formal training logs are retained and the e-learning training for budget holders was not mandatory but available to assist staff.

The Senior Financial Accountant also advised that all budget holders received induction training on budgets. We obtained the Finance for Non-Finance Managers PowerPoint presentation used for training and noted through review that the training included information on what are budgets, methods of budgeting, budget analysis, managing spend, and variances. We also noted that the training included steps on how to utilise Dream Finance system.

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.

Journals				
Control	Journals are raised and posted by the Finance Accountant with the reason for the journal recorded and no additional approval is required at this time. A report of all journals posted within the month is reviewed and independently authorised at month-end by the Finance Manager.		**Assessment:** **Design** ✓ **Compliance** ×	
Findings / Implications	We obtained a report of all journals posted from April to October 2022. Testing of a sample of 20 journals confirmed that, in all instances, there was backing documentation to support the appropriateness of the journal. A report of all journals posted in the month is generated and reviewed by the Finance Manager as part of the month-end activities. Review of the journal reports and month-end checklists for August, September and October 2022 confirmed journals had been subject to review by the Finance Manager or Senior Financial Accountant in a timely manner. However, we noted three instances in October 2022 where the Senior Financial Accountant prepared the journals and completed the month-end journal review. If journals are not independently reviewed, there is a risk that transactions may not receive the appropriate scrutiny challenge with may result in financial losses.			
Management Action 1	The Authority will ensure there is segregation of duties in the preparation and month-end review of journals.	**Responsible Owner** Finance Manager	**Date:** November 2022	**Priority:** Medium

For more information contact

Name: Suzanne 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