APPENDIX D

Business Assurance and Risk Management

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

Auditors

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

Selina Harlock, Audit Manager

Martin Baird, Mazar Director

Joseph Lennon, Mazars Associate Consultant

CONTENTS

Management Summary

Introduction

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

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

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

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

Audit Objective

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

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

Scope of work

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

- Logical Access Controls
- Change Controls
- IT Operations

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

Table 1: Overall Conclusion

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

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

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

Logical Access Controls

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

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

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

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

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

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

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

Change Controls

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

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

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

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

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

IT Operations

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

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

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

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

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

Table 2: Detailed Audit Findings and Management Action Plan

Finding 1: Service Reviews	Risk Rating	Agreed Management Actions
Service reviews are held monthly with the Vendor as part of the managed service contract. It was noted that no formal documentation is provided as part of these service reviews and these reviews are held informally with discussions over the telephone. No formal minutes or documents are retained by the Authority. In addition, the FSR system is cloud based and hosted on behalf of the Authority by the Vendor. Commonly in such scenarios, user organisations (i.e. the Authority) would proactively require independent assurances from the service provider (i.e. the Vendor) in order to provide comfort that those controls outsourced to the service provider by the user organisation operate effectively and continue to maintain effectiveness as IT risks change or emerge. The organisation is wholly reliant on the Vendor for the service provided without any assurances that risks and controls are being managed effectively. A risk that materialises in relation to the service provider environment could potentially have an impact on the Authority's reputation (e.g. a cyber breach at FSR could result in the Authority data leakage).	**H**	**Action:** Assurance to be sought from the vendor regarding efficacy of risk controls, especially in relation to cyber security. **Officer responsible:** Station Commander RMT **Date to be implemented by:** June 2021
Finding 2: Joiners, Movers and Leavers Policy/Procedure	**Risk Rating**	**Agreed Management Actions**
The Authority does not have a formalised user access management process outlining the processes/controls when a user joins, moves or leaves the organisation and the relevant user access requirements. We noted that: • When a joiner or mover requires new access or a change in access, a ticket is raised in the Vivantio service desk. Within this ticket, a 'child ticket' is sent to the Resource Management Team (RMT) to create/amend the user's access. • This ticket does not capture sufficient information for the RMT operator to provide access. • Often users will be provided access and then request further access as this has not been initially provided. Therefore, access being granted is an iterative process. • The lack of information on the ticket reduces the effectiveness of the audit trail. • Previously, when a user left the organisation, residual access could be left on the account, this is due to there being no formal procedure when revoking access. • The process has slightly changed whereby an operator will look at the user account to check what access they have before removing it. Unauthorised access to company resources may lead to loss and compromise of data.	**M**	**Action:** A review of the processes will be undertaken, supported by the end-to-end process mapping within the Internal Audit Plan for 2021-22. **Officer responsible:** Station Commander RMT **Date to be implemented by:** December 2021

Finding 3: Generic Accounts	Risk Rating	Agreed Management Actions
We inspected the user account list on FSR and noted that seven generic accounts exist on the FSR application as follows: • Five of these accounts have the username 'bucks_demoffX' where X is a number between 1-5. The use and rationale of these accounts was not provided by management; • One account with the username 'rmtcrashtestdummy' which similarly, was not rationalised; • One account has the username 'usardog'. It was noted that this account is created for the canine unit that the Urban Search and Rescue (USAR) team utilise. • It was further noted that the 5 'demoffX' accounts had never logged into FSR, the 'crashtestdummy' account was last accessed in May 2020. There could be a loss of accountability of user performed actions. Unauthorised access to company resources may lead to loss and compromise of data.	**M**	**Action:** A review of user accounts to be undertaken and redundant generic accounts to be removed. **Officer responsible:** Station Commander RMT **Date to be implemented by:** June 2021
Finding 4: Change Management - Testing	**Risk Rating**	**Agreed Management Actions**
The vast majority of change controls are operated by the Vendor. Irrespective, an internal change control process exists at the Authority. Changes are to be raised through the Vivantio service desk by a change initiator and must include key information However, we noted that: • The Authority does not have access to a test environment for FSR; • Changes are developed and tested by the Vendor; • Functional requirements and subsequent tender review for the application highlighted a question over access to a test environment to perform user acceptance testing (UAT) when a change is being made to the application; • Changes pass through over 1000 automated tests that are ran on the application to ensure that the change does not impact anything on the application, the change then has specific testing to ensure it is performing the functionality as per the design. • The Authority does not obtain any assurance from the vendor surrounding the change management process and is thus wholly reliant on the vendor for this. There is a risk that implementation of changes which are not aligned with business requirements and/or impact on the continued operation of the production application. Implementation of developments containing bugs or not matching the business' requirements.	**M**	**Action:** Change management process to be reviewed and fully documented (see also Finding 5). **Officer responsible:** Station Commander RMT **Date to be implemented by:** September 2021

Finding 5: Change Management – Internal Tracking and Assessment	Risk Rating	Agreed Management Actions
All changes are required to pass through the change management process with a request for change (RfC) document completed for each change. The Authority was unable to provide any documentation around the selected changes for inspection. Therefore, we were unable to determine if the change management process had been followed for the selected changes. This included cost benefit analysis and CAB minutes of discussion There is a risk of implementation of changes that contain bugs, misaligned with business requirements or impact on the continued operation of the production application. Development changes are misclassified, create unforeseen cost and/or are not assessed for business need and risk.	**M**	**Action:** Change management process to be reviewed and fully documented (see also Finding 6). **Officer responsible:** Station Commander RMT **Date to be implemented by:** September 2021
Finding 6: Backups – Disaster Recovery Testing	**Risk Rating**	**Agreed Management Actions**
Backups and the associated disaster recovery procedures are controlled and operated by the Vendor. Although it was determined that backups are being conducted on the FSR application and that the Vendor are trained to conduct disaster recovery tests, no evidence was available to inspect to demonstrate a disaster recovery test had been performed. We recognise that this is often an annual exercise and FSR has only been in effect at the Authority since April 2020. There is a risk of partial or complete loss of data. Unavailability of systems and lack of business continuity.	**M**	**Action:** A disaster recovery will be undertaken to test business continuity in this area. **Officer responsible:** Station Commander RMT **Date to be implemented by:** September 2021
Finding 7: User Access Reviews	**Risk Rating**	**Agreed Management Actions**
We noted that periodic user access reviews are not undertaken by the Resource Management Team at the authority when managing users access. Although a review of user access was completed in July 2020, there are no plans for this to continue. There is a risk of inappropriate access to the Authority's resources.	**L**	**Action:** User access to be reviewed every six months. **Officer responsible:** Station Commander RMT **Date to be implemented by:** September 2021

Finding 8: Password Configuration	Risk Rating	Agreed Management Actions
Fire service rota does not use traditional password configuration to manage passwords at a group level. FSR uses an 'entropy plugin' to set password configurations for all users which are set at 40 bits. Although 40 bits of entropy is considered 'reasonable' in regard to network and company passwords, full control over password parameters cannot be implemented as FSR (the application) does not allow for editing of password configuration. There is a risk of unauthorised access to company resources due to weak password configuration, which increases the likelihood of a brute force attack.	**L**	**Action:** Potential updating of the password configuration to be discussed with the supplier. **Officer responsible:** Station Commander RMT **Date to be implemented by:** March 2022

Appendix 1: Definition of Conclusions

Key for the Overall Conclusion:

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

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

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

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

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

Appendix 2: Officers Interviewed

The following staff contributed to the outcome of the audit:

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

The Exit Meeting was attended by:

Name:	Title:
Andrew Holtzhausen	Station Commander RMT

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

Appendix 3: Distribution List

Draft Report:

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

Final Report as above plus:

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

Audit Control:

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

Disclaimer

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

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

Contact Persons

Maggie Gibb, Head of Business Assurance

Phone: 01296 387327

Email: maggie.gibb@buckinghamshire.gov.uk

Selina Harlock, Audit Manager

Phone: 01296 383717

Email: selina.harlock@buckinghamshire.gov.uk