APPENDIX B

Business Assurance and Risk Management

BMKFA GDPR - FINAL (Ref-21/19)

Auditors

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

Selina Harlock, Audit Manager

Juan Fosco, Audit Manager

Nav Sidhu, Senior Auditor

CONTENTS

Management Summary

Introduction

The audit of the GDPR was undertaken as part of the 2020/21 Internal Audit plan, agreed by the Overview and Audit Committee. The audit was undertaken during quarter three of 2020/21.

The GDPR audit reviewed the Fire Authority's arrangements for data protection. It is vital to the achievement of the Fire Authority's strategic objectives to ensure that there are robust controls in place to adhere to regulations.

Audit Objective

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

This serves as a contribution towards the overall opinion on the system of internal control that the Chief Internal Auditor is required to provide annually. It also provides assurance to the Section 112 Officer that financial affairs are being properly administered.

Scope of work

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

- Compliance
- Roles and Responsibilities
- Records of Processing Activities (ROPA)
- Third-Party Management
- Retention and Destruction (including Systems and Technology)
- Management Information and Reporting

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

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
Compliance	**Reasonable**	**0**	**1**	**1**
Roles and Responsibilities	**Substantial**	**0**	**0**	**0**
Records of Processing Activities	**Reasonable**	**0**	**1**	**0**
Third-Party Management	**Substantial**	**0**	**0**	**0**
Retention and Destruction (including Systems and Technology)	**Reasonable**	**0**	**1**	**0**
Management Information and Reporting	**Partial**	**1**	**0**	**0**
		1	**3**	**1**

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

Compliance

The Authority has a Data Quality procedure which 'sets out processes to assure that information risks are being addressed adequately so that all data and information that is owned or managed by the Authority is accurate, available to Authority's people when needed, secured appropriately to prevent unauthorised access or alteration, and destroyed when no longer required'. The procedure was approved in January 2018. Discussions with the Information Governance and Compliance Manager confirmed the procedure is to be reviewed by the end of the financial year.

A Record Retention and Disposal/Information Assets Register (IAR) procedure is also in place. Its purpose is to ensure that the Authority holds records following legislation and business needs. This procedure was last reviewed and approved by the Head of Service Development in December 2019.

Other procedures are also in place, such as:

- Dealing with Requests for Information; and
- Redacting Sensitive Information.

However, our review identified that the 'Data Quality', 'Dealing with Requests for Information' and 'Redacting Sensitive Information' procedures referred to an Integrated Impact Assessment, which is no longer in place. It was also identified that the Redacting Sensitive Information procedure did not refer to when it was last reviewed and approved.

The Authority has a General Data Protection Regulation (GDPR) and a Cyber Security eLearning module implemented in April 2020. It runs at a two-year frequency for all staff. The People Systems and Learning Design Manager confirmed that as of December 2020, 103 (24%) staff members had completed both modules, and 324 (76%) had not.

Roles and Responsibilities

A Senior Information Risk Owner (SIRO) and a Data Protection Officer (DPO) are defined on the Authority's website. The roles and responsibilities of both are clearly defined in the procedures available to staff.

An Information Management Risk Register is in place which records GDPR risks and the ownership of each risk. Discussions with the DPO (who is the Information Governance and Compliance Manager) confirmed that the register is reviewed monthly to update risks identified within. Review of the Strategic Management Board (SMB) and Monitoring Board agendas confirmed that the review of the register is a standing item for both meetings.

Records of Processing Activities (ROPA)

Following the ICO's Accountability Framework guidance, ROPAs must, as a minimum, include:

- The organisation's name and contact details, whether it is a controller or a processor (and where applicable, the joint controller, their representative and the DPO);

- The purposes of the processing;
- A description of the categories of individuals and personal data;

We confirmed that a central ROPA spreadsheet is in place detailing the various processing activities undertaken. The central ROPA spreadsheet includes evidence of purpose, legal basis, and categories of individuals and information, in line with the ICO's Accountability Framework guidance.

Departments within the Authority are also responsible for retaining their ROPA spreadsheets. The Safeguarding's ROPA was reviewed. It was found that it did not specify whether it was a controller or a processor or the retention schedules.

Third-Party Management

Companies invited to tender are required to complete the Standard Invitation to Tender document, which includes preliminary questions regarding data protection and security. Any interested company has to confirm how it complies with GDPR legislation and should list the key actions undertaken to confirm compliance; it also has to confirm that data is held within the EU/UK. Additionally, standard wording is included in contract terms and conditions regarding confidentiality, data protection and GDPR.

We selected a sample of four contracts. We confirmed that the Standard Invitation to Tender document was completed in full by the companies. The respective contracts in place included the standard confidentiality, data protection and GDPR wording. The contracts reviewed were the following:

- Corporate Website;
- Incident Command Training;
- Fleet Management System; and
- Learning Management System.

Also, an e-form is used by the Procurement team to check compliance before approving to proceed with the tender/procurement process. The e-form includes, among others, a mandatory field to identify if the supplier/contractor processes personal information. If this is identified, the originator is referred to the DPO to seek further advice as to what additional documentation is required before setting up the new supplier/contract, such as a Data Protection Impact Assessment (DPIA). From the sample above, we identified that the Fleet Management System and Learning Management System required a DPIA. Testing confirmed that a DPIA was completed for both of these contracts.

Retention and Destruction (Including systems and Technology)

The Records Retention and Disposal Information Asset Register procedure states that information stewards are responsible for ensuring the timely archiving and/or destruction of records. They are also responsible for advising the information owners where it is believed a retention timescale should be amended following legislation or business needs.

The Information Governance and Compliance Manager is responsible for maintaining and reviewing records management processes. The retention schedules for departments and stations are defined within the ROPA. For paper documents, which have been archived, an archive master schedule is in place which states the retention period. Archive Centre Ltd manages the archived documents.

However, the Authority relies on information stewards to ensure that electronic data is disposed of (according to the retention schedule) and there is no mechanism in place to ensure this occurs.

The Authority's email system will address each email as it passes inbound or outbound from the servers. The system interrogates the email and attached documents looking for personally identifiable information, including but not limited to, EU Nation Identification numbers, Social Security Numbers or bank details. Once identified, the system generates an incident report passed to the ICT Service Desk for review and challenge users as to why they are sending the information.

Management Information and Reporting

The Business Transformation Board (BTB) terms of reference specify that one of the board's terms of reference is to review risks associated with change and that meetings are held monthly. We confirmed that meetings were held in June, August and September 2020. Also, quarterly Monitoring Board meetings occur where items such as directorate and corporate risks are discussed. Our review of meetings minutes from June to October 2020 confirmed that discussions around risks and GDPR took place and are being monitored.

During the audit fieldwork, the DPO confirmed that there had been no 'reportable breaches' at the Authority. The DPO noted that there had been three 'near misses' at the Authority between April and December 2020. One of which had been reviewed with investigations finalised and the remaining three were ongoing.

Our review of the investigation finalised found that a staff member had been granted inappropriate access to a certain folder. The access has been flagged before any reportable breaches. The report and investigation were documented using email trails.

After the audit fieldwork, a data breach incident was brought to Internal Audit's attention. The incident was related to an audit report for Staff Members' Equal Pay Report published within the Overview and Audit Committee agenda pack for the meeting dated 11 November 2020. Discussions with the Director of Finance and Assets confirmed that the report was accessed 20 times before being removed from the public website.

We confirmed that a documented investigation had been undertaken by the DPO raising 12 recommendations. The investigation raised a recommendation requiring HR to identify all employees whose personally identifiable information has been subject to inappropriate access and speak to the relevant Manager, who will be responsible for explaining to these employees that information has been released, measures taken, and those being taken to prevent further occurrences.

Table 2: Detailed Audit Findings and Management Action Plan

Finding 1: Data Incidents and Reporting	Risk Rating	Agreed Management Actions
Any data breaches/incidents at the Authority should be reported to the DPO and recorded in a data breach log along with lessons learned. Awareness should be regularly raised throughout the Authority regarding reporting of data breach incidents and lesson learned should be reported on at board meetings. During the audit fieldwork, the DPO confirmed that there had been no 'reportable breaches' at the Authority. However, after the audit fieldwork, a data breach incident was brought to Internal Audit's attention. The incident was related to an audit report for Staff Members' Equal Pay published within the Overview and Audit Committee agenda pack for the meeting dated 11 November 2020. Discussions with the Director of Finance and Assets confirmed that the report was accessed 20 times before being removed from the public website. An investigation was undertaken by the DPO raising 12 recommendations. The investigation required HR to identify all employees whose personally identifiable information has been published. Also, relevant Managers will be responsible for explaining that information has been released, measures taken, and those being taken to prevent further occurrences. If there is a lack of awareness of reporting for incidents, there is a risk that incidents are not identified and actioned promptly and a risk that reportable breaches are not reported to the ICO which may lead to fines.	**H**	**Action:** The recommendations of the DPO are currently being considered and further investigatory work is being undertaken. Actions will be determined once this work is complete. **Officer responsible:** Director of Finance and Assets **Date to be implemented by:** June 2021
Finding 2: E-learning modules	**Risk Rating**	**Agreed Management Actions**
E-learning modules are on an annual basis with rotation between the e-learning modules of GDPR and Cyber Security. The Authority has a General Data Protection Regulation (GDPR) and a Cyber Security eLearning module implemented in April 2020. It runs at a two-year frequency for all staff. The People Systems and Learning Design Manager confirmed that as of December 2020, 103 (24%) staff members had completed both modules, and 324 (76%) had not.	**M**	**Action:** Follow up with line managers of staff who are required to complete the training but have not done so within the specified time periods to ensure outstanding learning is completed. **Officer responsible:** Information

If an excessive period is granted to staff to complete training, there is a risk of an inconsistent approach to GDPR within the Authority, leading to breaches in legislation.		Governance and Compliance Manager **Date to be implemented by:** June 2021
Finding 3: Records of Processing Activities (ROPAs)	**Risk Rating**	**Agreed Management Actions**
ROPAs across all departments and stations are held in a digital catalogue accessible to the Information Governance and Compliance Manager; the catalogue should be linked to all individual ROPA's held within the Authority. The catalogue is used to complete compliance checks on ROPAs held across the Authority to ensure it meets ICO requirements. Departments within the Authority are also responsible for retaining their ROPA spreadsheets. However, the Safeguarding ROPA does not include all requirements stated by the ICO. This document did not specify whether it was a controller or a processor nor the retention schedules. If a centralised ROPA is held along with individual departmental ROPAs, the centralised ROPA is not kept up to date as the individual departmental ROPA's. If there is a lack of compliance checks, the risk of ROPAs not being kept up to date furthers.	**M**	**Action:** Agreed. ROPAs to be reviewed. **Officer responsible:** Information Governance and Compliance Manager **Date to be implemented by:** September 2021
Finding 4: Retention and Destruction	**Risk Rating**	**Agreed Management Actions**
The Records Retention and Disposal Information Asset Register procedure states that information stewards are responsible for ensuring the timely archiving and/or destruction of records and advising the Information Owners where it is believed a retention timescale should be amended following legislation or business needs. The Information Governance and Compliance Manager is responsible for maintaining and reviewing records management processes. The retention schedules for departments and stations are defined within the ROPA. The Authority relies on stewards to ensure that electronic data is disposed of per the retention schedule. However, there is no mechanism in place to ensure this takes place. If no adequate processes are in place to ensure lawful retention schedules and/or destruction of electronic records, there is a risk of accidental and/or unlawful alteration, destruction, or authorised personal data disclosure.	**M**	**Action:** Agreed. A mechanism to review data disposals inline with the retention schedules will be formalised and monitored. **Officer responsible:** Information Governance and Compliance Manager **Date to be implemented by:** December 2021

Finding 5: Procedures	Risk Rating	Agreed Management Actions
Policies and procedure should be reviewed regularly with revisions and approval dates recorded within each document. Review of procedures identified that the Data Quality procedure, Dealing with Requests for Information procedure and Redacting Sensitive Information Procedure referred to an Integrated Impact Assessment, which is no longer in place at the Authority. It was also identified that the Redacting Sensitive Information Procedure did not refer to when it was last reviewed and approved. Where policies and procedures are not reviewed regularly, there is a risk that staff guidance is not fit for purpose, which may lead to breaches in legislation.	**L**	**Action:** Agreed. Procedures will be reviewed and updated where necessary and review and approval dates updated. **Officer responsible:** Information Governance and Compliance Manager **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:
Gerry Berry	Information Governance and compliance manager
Dave Thexton	ICT Manager
Joanne Cook	Community Safety and Safeguarding Manager
Anne Stunnell	Head of Human Resources
Ronda Smith	Procurement Manager

The Exit Meeting was attended by:

Name:	Title:
Gerry Berry	Information Governance and compliance manager
Dave Thexton	ICT Manager
Joanne Cook	Community Safety and Safeguarding Manager
Anne Stunnell	Head of Human Resources

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:

Gerry Berry	Information Governance and compliance manager
Dave Thexton	ICT Manager
Joanne Cook	Community Safety and Safeguarding Manager
Anne Stunnell	Head of Human Resources
Mark Hemming	Director of Finance and Assets

Final Report as above plus:

Jason Thelwell	Chief Fire Officer
Ernst and Young	External Audit

Audit Control:

Closing Meeting	16 December 2020
Draft Report	2 February 2021
Management Responses	23 February 2021
Final Report	24 February 2021
Audit File Ref	21-19

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