Internal Audit Report

Data Protection

Report distribution:

Martina Doolan – Data Manager
Kash Singh – Strategic Enabler Digital and Data
Gary Taylor – Assistant Chief Fire Officer & SIRO

Report no: FS306
Date issued: July 2021

Contents:

1 Executive summary

Introduction

An audit Data Protection was undertaken as part of the approved Internal Audit Plan for 2020/21.

Scope and objectives of audit work

Our audit considered the objectives and the potential risk to the achievement of those objectives.

Objectives Reviewed	Potential Risks
To provide assurance that the necessary safeguards are in place to ensure the appropriate use of personal and corporate information.	• Data breaches are not managed appropriately. • Risks are not identified, or controls and actions put in place to mitigate them.
Limitations to scope of audit	Limited to recent subject access requests and data breaches.

Overall conclusion

	Limited	Satisfactory	Substantial
Our audit provides **Substantial Assurance** over the adequacy of the controls reviewed as part of the process to mitigate risks to an acceptable level.	There is a risk of objectives not being met due to serious control failings.	A framework of controls is in place, but controls need to be strengthened further.	There is a robust framework of controls which are applied continuously.

Key issues identified

We have identified one significant issue where improvement could be made, arising from the following:

- Assurance cannot be provided that subject access requests are responded to within specified deadlines.

Suggested actions for identified issues are shown in the main body of the report. The key issues arising from this report may be included in summary form to the Audit and Risk Committee.

2 *Issues arising*

Action is required to avoid exposure to significant risks in achieving objectives **Significant**		
No	**Issue arising**	**Agreed action including responsibility and target date**
2.1	A sample of five Subject Access Requests (SARs) was selected to be examined to ensure compliance with required deadlines. However, for three of the sample (SARS20002, SARS20003 and SAR20004), no documentary evidence was provided during this review to enable timescales to be confirmed. **Implication:** Assurance cannot be provided that SARs are responded to within required deadlines.	Documentary evidence should be retained for all SAR requests to demonstrate compliance with required deadlines. Management response: Automated techniques using Office 365 E-Discovery tools being assessed which will provide case management functionality and audit trail. Deadline and Responsible Officer: 31 October 2021 – Data and Governance Manager

Action is advised to enhance risk control or operational efficiency **Merits Attention**		
No	**Issue arising**	**Agreed action including responsibility and target date**
2.2	Monthly reports are produced and presented to the Strategic Enabling Team (SET) which detail the number of Subject Access Requests (SARs) and Freedom of Information Requests (FOIs) received by the Authority, and how many have been responded to within a specified time frame. The reports presented to SET contained errors. For example, the March report for 2020 illustrated that one SAR had been received by the Authority when in fact three had been received. **Implication:** Incorrect position is being presented to SET with regards to SARs received and responded to.	Reports presented to SET should be checked to ensure that they contain the correct information. A reconciliation should be undertaken between the monthly report produced to SET compared to the recording spreadsheet for before reports are submitted to the SET meeting. Management response: This issue of time lag and missing entries has been remediated. The Strategic Enabling Team (SET) have access to a Power Bi dashboard showing Data Protection Subject Access Requests (SAR) and Freedom of Information (FOI) requests as soon as they are logged within the Data and Governance Team. Deadline and Responsible Officer: Complete circa January 2021 – Data and Governance Manager

Limitations inherent to the internal auditor's work

This report has been prepared solely for the authority in accordance with the terms and conditions set out in the terms of reference. Internal audit does not accept or assume any liability of duty of care for any other purpose or to any other party. This report should not be disclosed to any third party, quoted or referred to without prior consent. Internal audit has undertaken this review subject to the limitations outlined below.

Internal control

- Internal control systems, no matter how well designed and operated, are affected by inherent limitations. These include the possibility of poor judgement in decision making, human error, control processes being deliberately circumvented by employees and others, management overriding controls and the occurrence of unforeseeable circumstances.

Responsibilities of management and auditors

- It is management's responsibility to develop and maintain sound systems of risk management, internal control and governance for the prevention and detection of irregularities and fraud. Internal audit work should not be seen as a substitute for management's responsibilities for the design and operation of these systems.
- Internal audit endeavours to plan audit work so that it has a reasonable expectation of detecting significant control weakness and if detected, will carry out additional work directed towards identification of consequent fraud or other irregularities. However, internal audit procedures alone, even when carried out with due professional care, do not guarantee that fraud will be detected.
- Accordingly, these examinations by internal auditors should not be relied upon solely to disclose fraud, defalcations or other irregularities which may exist.