FOI11388: Annex A

Please see below extracts from Audit Committee papers that reference our own compliance with GDPR during the period 1 April 2023 to 31 March 2024.

AuditCo 20230519 - Item 10ii Recommendation for committee ownership of Internal Audit themes

Audit Committee

Date of meeting: 19 May 2023

Subject Recommendation for committee ownership of Internal Audit themes

Annex 1: IA themes and proposed committee ownership

Grouping	Theme (identified by IA)	Description of theme	Proposed Committee
Information Security	Weaknesses in key controls resulted in the provision and publication of personal information	As a public body and regulator that protects consumers and takes action against firms and individuals, it is important the FCA complies with the law. Non-compliance can cause harm to consumers, damage the FCA's reputation, and distract the FCA from delivering its objectives. The Internal Audit Division conducted two reviews which found that the provision of personal information to a third party in one instance and the publication of personal information in two instances were the result of weaknesses in key controls. The QA performed in both	RiskCo

		reviews did not identify that personal information would be published. This was because the quality of the QA performed was below the standard required for management to rely on QA as a preventative control. The review of information in the sign off process was also deficient as information in hard copy was reviewed as opposed to information that would have been provided electronically. The quality and frequency of training supplemented by the effective supervision of staff responsible for ensuring that personal data is not published were also deficient. Staff responsible for these tasks are not alert to the possibility that personal information may be shared because the staff responsible were junior, had not been trained and were not adequately supervised. In addition, the quality of general training on Data Protection is limited as it does not sufficiently identify the risks of mishandling personal information and the controls that should be in place. In both instances reported below, it was	

		not the FCA control environment that identified the breach of DPA and GDPR. Instead, the FCA was notified of these breaches by external parties. These issues point to a broader issue in that there is limited appreciation of the risks associated with key activities where personal information is collected and used in the ordinary course of work. While the organisation knows how to treat/handle non-personal information, more needs to be done to improve the understanding of how to treat/handle personal information and the need for effective controls.	

AuditCo 20230713 - Item 07 - Compliance Report Plan and KRI Paper FINAL

Audit Committee

Date of Meeting: 13 July 2023

Subject: COMPLIANCE OVERSIGHT – PLAN AND REPORTING UDPATE

2 Proposal Outcomes and Success Measures
2.1 Having laid the foundations of the enhanced function in 2022/23; the key activities in the 2023/24 Compliance Plan are designed to drive a further culture shift, enabling and supporting the first line in delivering compliance management by:
e. Baselining the FCA and PSR's data protection risk profile as the DPO function and commencing remediation of any gaps.

AuditCo 20230713 - Item 07 - Annex 1

Annex 1 –The Compliance Oversight Plan for 2023/2024

Outcomes	Q1	Q2	Q3	Q4
Deliver a DPO Function that is fit for purpose and drives up standards	Deliver DPO function in RCO	Baselining of FCA and PSR Data Protection Compliance	Baselining of FCA and PSR Data Protection Compliance	Continue remediation

Joint meeting of the FCA and PSR Audit Committees 20230914
Item 05 - Annex B

Annex B – Executive summary of the Data Subject Access Requests review
Financial Conduct Authority

Internal Audit report

Data Subject Access Requests

10 August 2023

1 Summary

1.1 Executive Summary

Key findings

At the start of 2022, the FCA had a significant and increasing backlog of overdue DSAR cases many of which were significantly beyond the required one-month response time for non-complex, routine cases.

In January 2022, an interim Manager was brought in to provide oversight and an external legal firm was engaged to support the team in eliminating the backlog of breached cases.

The support obtained from the external law firm and new staff recruited helped to clear the DSAR backlog by the end of 2022, from a peak of 59 cases in breach in April 2022 to 1 case in breach in August 2022. This position has been maintained and at the start of 2023, FCA DSAR responses were being provided within defined service levels.

Conclusion

The current DSAR approach is highly reliant on staff who, although they have significant Data Protection and DSAR knowledge and experience, are new to the FCA and who do not have a clear documented structure to follow in respect of how DSARs should be handled and how relevant legal provisions and exemptions are to be applied in practice at the FCA.

external law firm support was provided to assist in clearing the backlog of overdue DSAR responses.

1.2 Overall management comments

During this period of flux, I would like to acknowledge the work the DSAR teams have done. They currently have no backlog of cases and are within service level.

FCA and PSR AuditCo 20240314 Item 08 - Compliance Plan 2023_24 Update

FCA & PSR Audit Committee (AuditCo)

Date of meeting: 14 March 2024

Subject: COMPLIANCE PLAN 2023/24 UPDATE

Data Protection Update
4.6 The newly appointed DPO conducted a high-level gap analysis of the FCA's approach to compliance with the UK GDPR and Data Protection Act against the ICO's own standards. This review indicates that there is work to be done to strengthen our compliance. Following this work, and as part of Business Planning, ExCo agreed the recruitment of five heads, recruitment of whom is underway. The main focus for this resource will be initially: to update and restate the FCA's record of processing activities; establish a formal DP complaints handling process; design a training programme and offer bespoke training to higher risk areas of the FCA; and provide a more consistent DPO advisory function.

FCA and PSR Audit Committee - 20240314 Minutes Draft

Minutes

Meeting: Joint Meeting of the FCA and PSR Audit Committees

Date of Meeting: 14 March 2024

8.3 AuditCo asked about the data protection function not advancing in line with data expansion and how the FCA would address the gaps against the Information Commissioner's Office (ICO) standards. In response the Committee heard that mapping of personal data was a priority and were advised that the Head of Compliance role now incorporated the role of Data Protection Officer (DPO), and that this role would address the gaps identified.

8.4 The Chair summarised that:
b. Data protection would need to be tracked and brought to AuditCo with information on the DPO's activity.

	Description	**Owner**	**Sponsor**	**Deadline**
Action	Provide enhanced detail and update of the Data Protection Officer current and future work to address the compliance gap against ICO standards with the next compliance plan update.	Joe Usher	Stephen Braviner Roman	11/07/2024

FCA AuditCo 20240314 Chairs Report

FCA Board Committee Chair's Report

1. Name of Committee: Joint Meeting of the FCA and PSR Audit Committees

2. Committee Chair: Liam Coleman

3. Date of meeting: 14/03/2024

5. Key discussion items to highlight:

c. AuditCo discussed how the compliance plan could ensure change rather than merely addressing capacity, the risks of data protection not keeping up with data expansion, and the targeting of policy reviews in the most impactful and problem areas. AuditCo requested a further data protection update to understand the work of the Data Protection Officer in addressing the work to strengthen FCA compliance against UK GDPR and the Data Protection Act.