Devon and Cornwall Police and Dorset Police

Follow-up data protection audit report

September 2021

Information Commissioner's Office

Executive summary

Background

The Information Commissioner is responsible for enforcing and promoting compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA18) and other data protection legislation. Section 146 of the DPA18 provides the Information Commissioner's Office (ICO) with the power to conduct compulsory audits through the issue of assessment notices. Section 129 of the DPA18 allows the ICO to carry out consensual audits. The ICO sees auditing as a constructive process with real benefits for controllers and so aims to establish a participative approach.

Devon and Cornwall Police and Dorset Police (DCP and DP) agreed to a consensual audit by the ICO of its processing of personal data.

The audit was conducted following the Information Commissioner's data protection audit methodology. The key elements of this were a desk-based review of selected policies and procedures, on-site visits including interviews with selected staff, and an inspection of selected records.

However, due to the outbreak of Covid-19, and the resulting restrictions on travel, the on-site visit was not possible, and interviews were conducted with selected staff on a remote basis.

The original audit took place remotely between 8 and 10 September 2020 and covered the following scope areas:

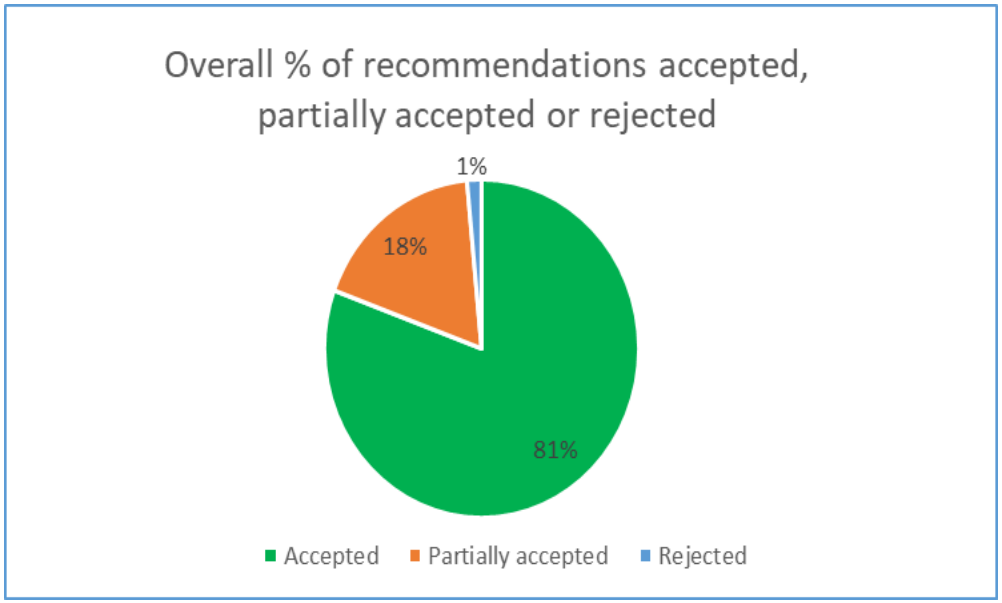
Scope Area	Description
Governance and Accountability	The extent to which information governance accountability, policies and procedures, performance measurement controls, and reporting mechanisms to monitor data protection compliance to both the GDPR and national data protection legislation are in place and in operation throughout the organisation.
Requests for Access to Personal Data	There are appropriate procedures in operation for recognising and responding to individuals' requests for access to their personal data.
Personal Data Breach Management and Reporting	The extent to which the organisation has measures in place to detect, assess and respond to security breaches involving personal data, to record them appropriately and notify the supervisory authority and individuals where appropriate.

Where weaknesses were identified recommendations were made, primarily around enhancing existing processes to facilitate compliance with the DPA.

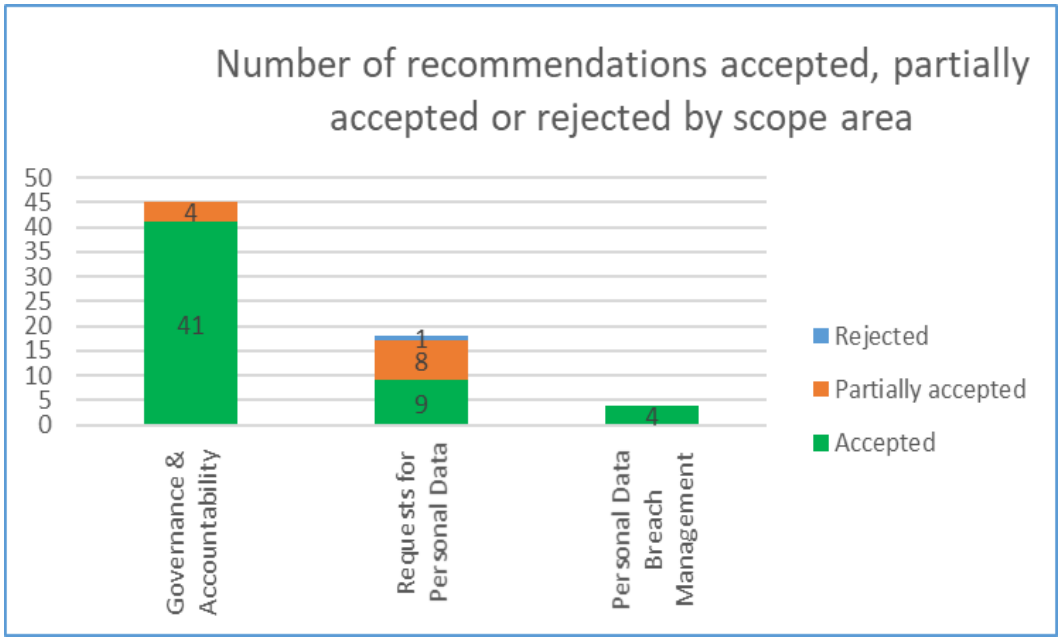
A total of **67** recommendations were made in the original audit report. In order to assist DCP and DP in implementing the recommendations each was assigned a priority rating based upon the risks that they were intended to address. The ratings were assigned based upon the ICO's assessment of the risks involved.

DCP and DP responded to these recommendations positively, agreeing to formally document procedures and implement further compliance measures.

The following charts summarise DCP and DP's response to the recommendations made.



The pie chart above shows that overall, **81%** of recommendations have been accepted, **18%** have been partially accepted and **1%** have been rejected.



The bar chart above shows that for the Governance & Accountability scope, **41** recommendations have been accepted and **4** have been partially accepted.

For the Requests for Personal Data scope, **9** recommendations have been accepted, **8** have been partially accepted and **1** has been rejected.

For the Personal Data Breach Management scope, all **4** recommendations have been accepted.

Follow-up process

The follow up audit consisted of three stages; the first interim follow up audit which took place in February 2021, four months after the final report was issued, the second interim follow up in June 2021 and the final follow up audit conducted in September 2021, 11n months after the final audit report was published and the engagement concluded. All stages of the follow up audit are desk-based exercises.

The primary aim of the interim follow up is to establish how much progress has been made with addressing the urgent and high priority recommendations, and to understand what the challenges are to completing them. The objective of a follow-up audit assessment is to provide the ICO with a level of assurance that the agreed audit recommendations have been appropriately implemented to mitigate the identified risks, and thereby support compliance with data protection legislation and implement good practice.

For all Urgent and High priority recommendations made in the original audit report, DCP and DP are required to provide an update on the actions they have taken with supporting documentation to evidence progress.

For all Medium and Low priority recommendations made in the original audit report, DCP and DP are required to provide an update on the actions they have taken.

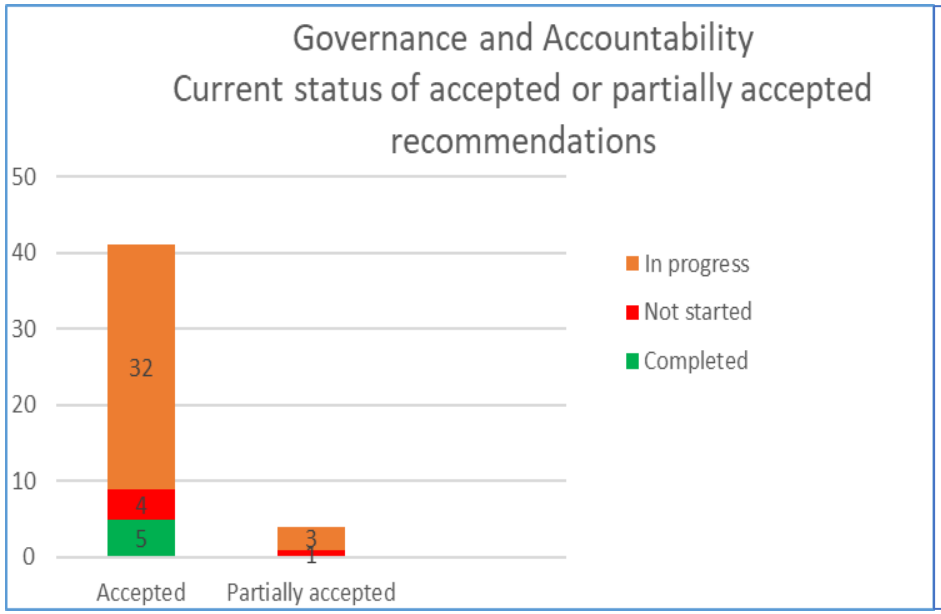
The updated Action Plan at the final follow up audit should be signed off at Board Level.

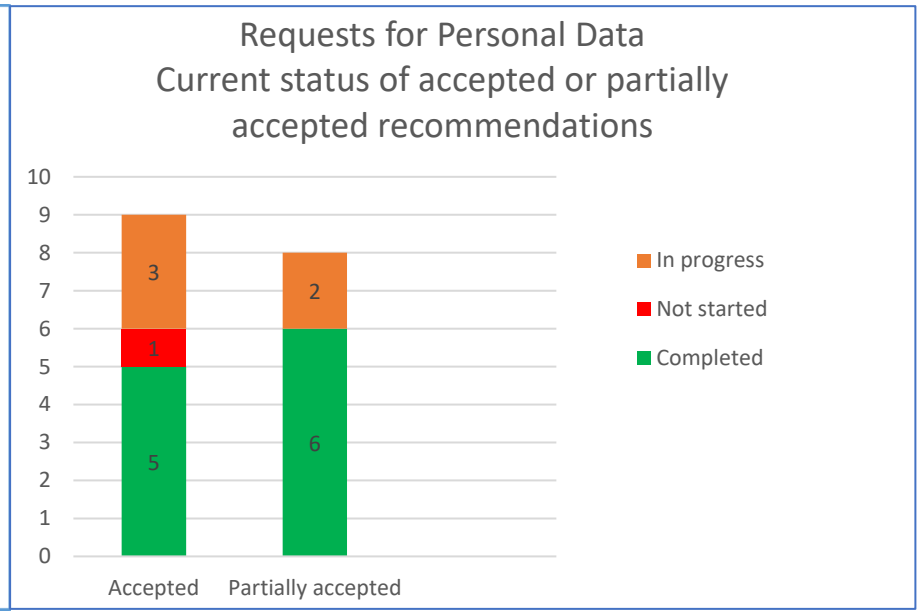
Interim Follow-ups

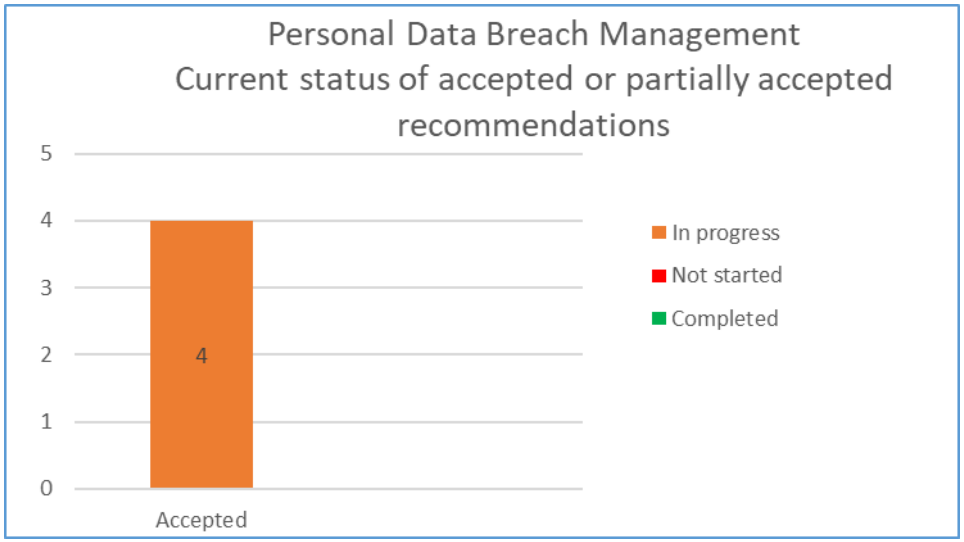
During the interim follow ups, DCP and DP had demonstrated some progress with addressing the non-conformities and recommendations accepted and partially accepted, in the final data protection audit report.

Follow-up audit summary

A desk based follow-up audit took place in September 2021 to provide the ICO and DCP and DP with a measure of the extent to which DCP and DP had implemented the agreed recommendations. The following charts show a summary of progress to date.

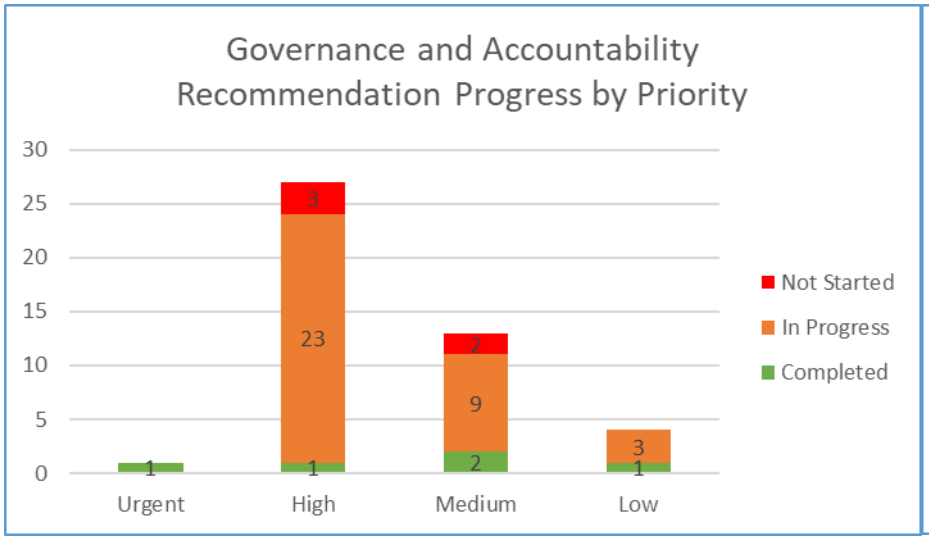


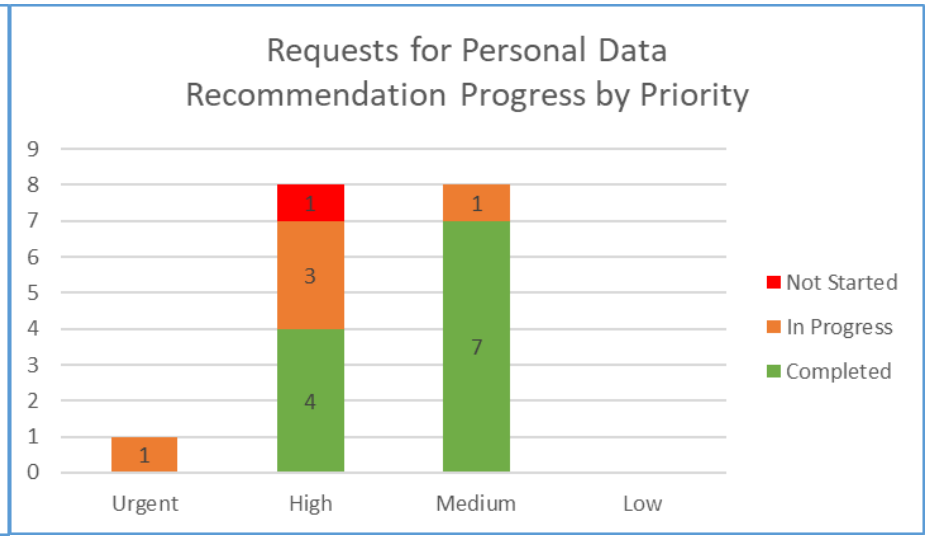


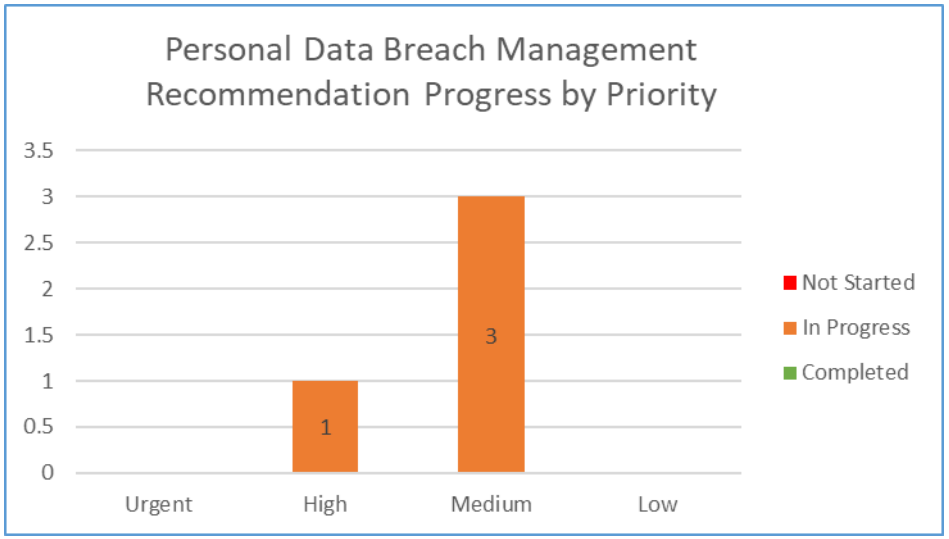


- In the Governance and Accountability scope area **5** recommendations have been completed, there are still **35** recommendations in progress and **5** that have not yet been started. Of the 5 that have not yet been started, **3** are rated as High Priority recommendations.
- In the Requests for Personal Data scope area **11** recommendations have been completed, **5** are in progress with **1** that has not yet been started.
- In the Personal Data Breach Management scope area all **4** recommendations are in progress.

  In these instances there remains the residual risk of non-compliance with data protection legislation.


Governance and Accountability
Recommendation Progress by Priority
30
25
20
15
10
5
0
Urgent
High
Medium
Low
1
1
23
3
2
9
2
3
1
Not Started
In Progress
Completed


Requests for Personal Data
Recommendation Progress by Priority
9
8
7
6
5
4
3
2
1
0
Urgent
High
Medium
Low
1
4
3
1
7
1
Not Started
In Progress
Completed


Personal Data Breach Management
Recommendation Progress by Priority
3.5
3
2.5
2
1.5
1
0.5
0
Urgent
High
Medium
Low
1
3
Not Started
In Progress
Completed

- In the Governance and Accountability scope area we are pleased to note that the urgent priority recommendation has been completed. However, only **1** high priority recommendation has been completed, **23** are still in progress and **3** have not yet been started. This accounts for **58%** of the accepted/partially accepted recommendations in this scope area not completed.
- In the Requests for Personal Data scope area we note the urgent priority recommendation is still in progress. Of the **8** high priority recommendations only **4 (50%)** have been completed, **3** are in progress and **1** has not yet been started.
- In the Personal Data Breach Management scope area we note that the high priority recommendation action is still in progress.
- Across all three scope areas **66** recommendations were accepted/partially accepted. **38 (58%)** of those were urgent/high priority recommendations, **24** (**36%**) were rated medium priority and 4 (**6%**) rated as low priority.
- A total of **4** high priority recommendations have not been started.

In these instances there remains the residual risk of non-compliance with data protection legislation. DCP and DP had not provided definitive timescales for completion of the remaining actions at the time of this follow up report.

Key follow-up audit findings

Main improvements include:

- Appropriate Policy Documents (APDs) are in place to show that the processing of sensitive/special category data is compliant with the requirements of Article 9 of the UK GDPR and section 42 of the DPA18.
- Induction training presentations for both DCP and DP have been updated and aligned to ensure that it is consistent across the Alliance; and that staff are made aware of the additional requirements associated with special category data and the additional risks and impact of a personal data breach. In addition, training needs have been identified for staff with specialised roles within the Information Management department.
- A review of Privacy Notices has taken place to include an "Easy Read" version and to ensure that operational staff are aware of where to direct members of the public for detailed privacy information.
- DCP and DP have created template letters to provide data subjects with more detail where their request is deemed or assessed as manifestly unfounded or excessive.

Main risk areas still outstanding:

- DCP and DP have amended their Information Asset Register (IAR)/Record of Processing Activities (RoPA) template however they are yet to roll out the IAR/RoPA for all departments to complete. They are not compliant with Article 30 of the UK GDPR and Section 61 DPA18. DCP and DP have made some progress with IAR/RoPA but operational pressures and conflicting priorities have resulted in the delay.
- Privacy Notices and APDs still require updating in line with the completed IAR/RoPA. No further timescales for completion of the IAR/RoPA have been provided.
- Compliance checks to ensure that staff are understanding and following Information Governance (IG) policies and procedures have yet to be formally implemented. They are not compliant with its responsibilities under UK GDPR Articles 24 and 5(1)(f) and 5(2).

- DCP and DP have started but not completed the review of the data processor contracts they have in place. DCP and DP should ensure that compliance checks on processors are implemented and establish how contact will be made with processors who may hold personal data that is required to respond to a right of access request under Article 15 of the UK GDPR and Section 45 DPA18.
- DCP and DP have not completed their review of where consent is being relied upon as a lawful basis for processing personal data. They plan to complete the review when the IAR/RoPA is rolled out to all areas.
- DCP and DP's Data Protection Policy is scheduled for review at the same time as this follow up audit. DCP and DP have yet to update their working practices with information on the correct exemptions to apply as part of that review. DCP and DP should ensure that they schedule cold case reviews of SAR responses.
- DCP and DP still have a significant number (some historical) in the backlog for subject access requests which exceed the statutory timescales as set in the UK GDPR and Part 3 DPA18, for responding to the Data Subject. The ICO and DCP and DP are continuing to monitor their progress in responding and the causes affecting their ability to respond within the statutory timescales.
- DCP and DP have yet to implement a retention period for emails.

In addition to the risks referred to above with regards to some of the completed recommendations (for example A.11)we asked for evidence of minutes of meetings, emails and actions, however either minutes were not taken, emails could not be located and actions not detailed. DCP and DP should ensure that actions/decisions are appropriately documented. This will assist with complying with the Accountability Principle.

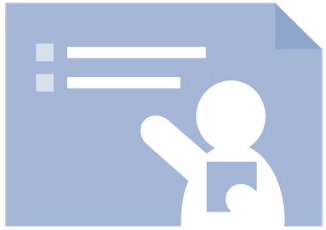
DCP and DP should also ensure that in responses to subject access requests the lawful basis being relied upon should be granular and specific.

Further detail on the recommendations in progress and not started can be found in the attached action plan.

Follow-up audit conclusion

We acknowledge the progress DCP and DP is making towards the completion of the actions for the original recommendations against the scope areas, having completed **16 (25%)** of the total **66** recommendations accepted/partially accepted. However, there is still progress to be made in areas where a continued residual risk remains including **44** actions partially completed **(66%)** and **6** not started **(9%)**. DCP and DP have not provided further timescales for the completion of the actions and recommendations. Therefore, we would suggest that DCP and DP revisits these recommendations and actions, sets new completion dates where the original date has not been met and considers whether the priority of an action should change based on time passed. DCP and DP should take urgent steps to review and complete all the actions as agreed in the original audit report, failure to control the risks identified by our audit of DCP and DP may result in non-compliance with data protection legislation and serious personal data breaches.

Credits



ICO Auditor

Sheryl Lewis – Lead Auditor

Thanks

The ICO would like to thank Richard Scott, Alliance Information Compliance Manager for their help in the audit follow up engagement.

Distribution List

This report is for the attention of Michael Stamp - Director of Legal Reputation and Risk and Senior Information Risk Owner, Louise Fenwick - Head of Information Management, Richard Scott – Alliance Information Compliance Manager, Tracey Furbear – Data Protection Officer (Devon and Cornwall Police) and Sean Walbridge – Data Protection Officer (Dorset Police).

Disclaimer

The matters arising in this report are only those that came to our attention during the course of the follow up audit and are not necessarily a comprehensive statement of all the areas requiring improvement.

The responsibility for ensuring that there are adequate risk management, governance and internal control arrangements in place rest with the management of DCP and DP.

We take all reasonable care to ensure that our follow up audit report is fair and accurate but cannot accept any liability to any person or organisation, including any third party, for any loss or damage suffered or costs incurred by it arising out of, or in connection with, the use of this report, however such loss or damage is caused. We cannot accept liability for loss occasioned to any person or organisation, including any third party, acting or refraining from acting as a result of any information contained in this report.

This report is solely for the use of DCP and DP. The scope areas and controls covered by the original audit were tailored to DCP and DP and, as a result, this report is not intended to be used in comparison with other ICO follow up audit reports.