1. Executive Summary

1.1 This paper summarises the third annual data protection assurance report for Social Security Scotland. It covers findings of dedicated data protection assurance activity carried out in 2023-24 as well as compliance findings from other data protection activities.

1.2 Key findings of this year's report are:

- business areas have continued to develop and rely on ad hoc process development without data protection impact assessment which risks processing of personal data out of compliance with data protection legislation (section 2).

- data protection impact assessments transitioning from Programme have required significant rework to reflect current operational practice and address gaps in governance and risk management. This is a contributing factor to some of the risk management concerns identified in data protection health checks (section 3).

- there have been no instances identified of data sharing with or data processing by third parties without appropriate measures in place in initiatives originated by Social Security Scotland. This suggests collaboration between responsible teams and processes to identify data processing in procurement initiatives are effective (section 4).

- numbers of data subject requests have increased significantly as the client base has increased and adverse decisions have been made on benefit applications. Social Security Scotland processes do not currently allow for ease of access by clients to their personal data, meaning clients are submitting requests under their right of access (section 5).

- breaches related to client addresses in Social Programme Management (SPM) continue to be the overwhelmingly largest category of breach. These have multiple root causes and varying effects (section 6).

- there is evidence of an embedded culture in incident awareness and reporting which supports a continuous improvement approach (section 6).

2. Data Protection Health Checks – Summary of Findings

2.1 The Data Protection Officer agreed that for the reporting year 2023-24 assurance activities should review the handling of personal data by all core business areas involved in the processing of Child Disability Payment, having focused on data protection issues in low income benefits in 2022-23.

2.2 The findings of health checks conducted in 2023-24 were consistent with health checks conducted in previous years. There is a significant dependency on using MS Excel to create tools to track workflow and produce management

information as functionality within SPM system was inadequate for the business areas' requirements. Each business area had created their own processes and Information Technology (IT) tools for controlling workflow and recording activities. There was evidence of some useful best practice and IT tool development, but this had not been shared amongst the business areas.

2.3 A common theme was that no information risks were held on business areas' risk registers. All of the business areas had developed local work processes that were not articulated in any design documents originating from Social Security Programme and consequently the application of the data protection principles to these processes had not been considered. This has led to significant volumes of personal data being created or duplicated with minimal controls regarding retention and other matters.

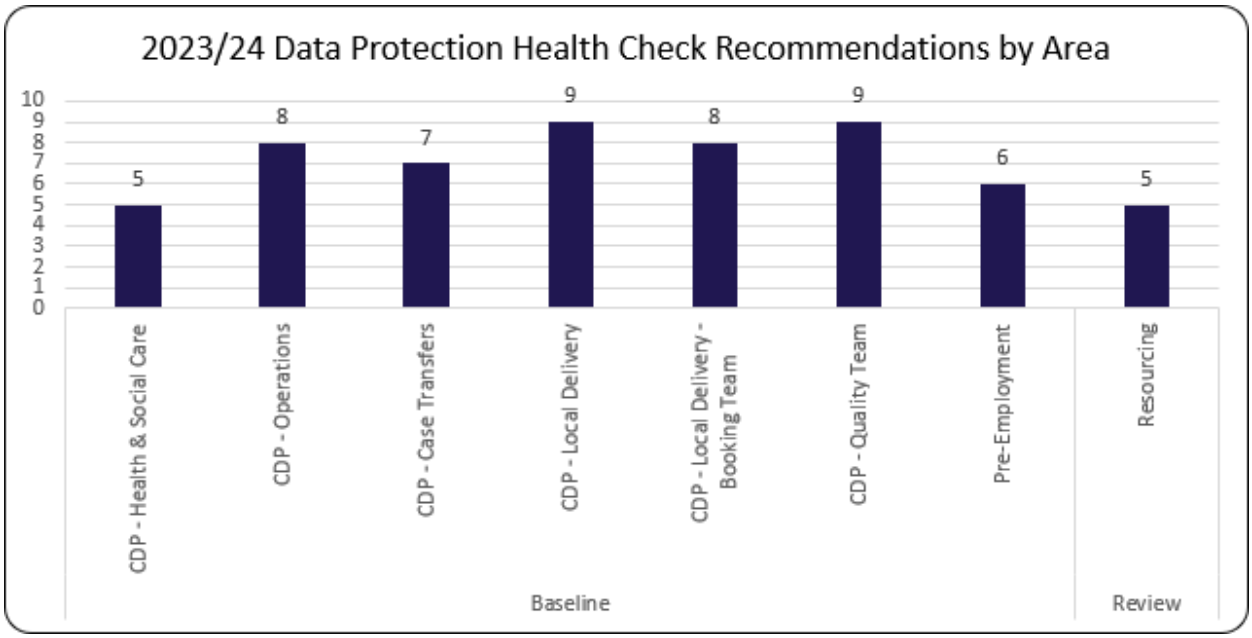
2.4 The baseline health checks conducted by the data protection assurance team have been further developed during this reporting year by making use of the analysis of issues identified through personal data breach investigation. This allowed for more informed targeted activities to be undertaken to provide a greater degree of confidence in the findings.

2.5 This reporting year has seen the introduction of health check reviews. These are designed to establish what activities have been undertaken to address the recommendations made in previous years' health checks, and to establish if any additional working practices have been developed in the business areas subsequent to the original health check that involve processing of personal data. There have been mixed findings with some business areas addressing most of the baseline health check recommendations, but engagement with others has shown minimal action has been undertaken to address the recommendations. The reviews will be an area to further develop in the next reporting year including how they will align with the transition of products .

2.6 The team now routinely gathers feedback from the business areas regarding the engagement throughout the health check process. This has been overwhelmingly positive. Business area suggestions provided in feedback on the assurance approach have now been considered and implemented as part of a continuous improvement approach to the assurance activities.

2.7 The collaborative approach adopted by the data protection assurance team has led to closer working with a number of business areas and this has resulted in additional data protection impact assessments being completed. There has been ongoing support provided to business areas who have approached the team for advice and guidance before adopting any changes to processes. This indicates that there is a greater awareness of the data protection principles that need to be considered and that some business areas are actively seeking guidance on handling personal data as a result of assurance engagement.

Figure 1: Data Protection Health Check Recommendations



2.8 Common issues identified from health checks in 2023-24 were that:

- business areas continue to demonstrate some awareness of data protection requirements, but identification and management of risks to compliance was lacking;

- business areas are continuing to create tools, trackers, and databases, which can hold significant volumes of personal data, without ensuring the design and operation of these take account of data protection requirements. There are a number of risks associated with this activity that are not being captured and managed;

- there are often insufficient controls and governance for reviewing access and appropriate retention of personal data held in the organisation's systems [redacted] The principal area requiring attention is reviewing [redacted] Creating new user accounts [redacted] although new processes in some areas have contributed to mitigating this risk; and

- there was evidence of personal data being collected or duplicated without adequate appropriate business reasons. This is likely to present issues in compliance with data protection requirements (for example, in meeting the storage limitation, accuracy and integrity and confidentiality principles and in complying with data subject rights requests). This indicates a continuing requirement for guidance and training on such issues to enhance application of the requirements of data protection legislation and organisational policy.

3. Data Protection by Design

3.1 The Data Protection and Information Governance branch has supported colleagues with Data Protection Impact Assessments on personal data processing initiatives in corporate activities.

3.2 Data Protection Impact Assessments and associated artefacts concerning Client Service Delivery products have been the responsibility of the Social Security Programme's Information Governance team until now. In the 2023-24 plans to transfer these artefacts were finalised and subsequently approved by the Senior Transition Project and respective Programme and Social Security Scotland leads.

3.3 Formal handovers commenced in January 2024. Responsibility and accountability for all low income benefit data protection impact assessments and data sharing agreements have now formally transitioned. There has been some positive engagement with product owners which has helped to further embed a data protection by design culture into our services. Most of the data protection impact assessments inherited from Programme require a significant amount of rework to ensure they reflect current personal data processing and that information risks are properly identified and managed. This is a contributing factor to some of the risk management concerns identified in data protection health checks about the creation of new processes which have not been subject to data protection impact assessment. These issues are in part caused by the time between the documents transitioning and lack of ownership and understanding of the responsibility of Product Owners for the management of data protection impact assessments.

3.4 Relationship management with external partners including the Department for Work and Pensions, HM Revenue and Customs and the Department for Communities (Northern Ireland) is a key feature of the handover process to ensure the effective maintenance and review of the data sharing agreements which underpin the delivery of our benefits. Engagement with all parties has commenced and discussions on future ways of working are underway.

3.5 Handover phases have been planned until the end of 2024-25 and the artefacts that will fall within scope of each phase is considered in advance. The objective for this year to transition all data protection impact assessments and associated artefacts for products which have transitioned to agency allowing us to align with product transition thereafter. The working relationship between the Social Security Scotland and Programme teams is formalised in a Memorandum of Understanding.

3.6 The Data Protection Officer continued to advise on and review Data Protection Impact Assessments originating from both Social Security Scotland and the Social Security Programme.

3.7 Health checks have continued to indicate that processes in benefit delivery have evolved to meet business needs in ways which have not been subject to a formal data protection impact assessment. Health checks have also identified that corporate functions (and others whose development was not supported by Programme) have similarly not been subject to data protection impact assessment.

This means that it is likely that processing of personal data in these functions may be at risk of non-compliance with data protection legislation. Health checks have recommended actions to address these gaps with the support of the Data Protection Team.

4. Third Party Risk

4.1 Third party risk concerns risk to personal data processed by or shared with third parties (typically suppliers who are contracted to provide services, including data processing services, or other public bodies with whom Social Security Scotland exchanges personal data for our core functions). The Data Protection Team, Procurement and Commercial and Digital Risk and Security implemented an enhanced process in August 2023 for reviewing new procurement initiatives to identify and record relevant data protection and information security considerations. This process embeds data protection impact assessment screening questions as a default when requests for procurement assistance are made, leading to engagement on data protection requirements at the early stages of each notified procurement initiative.

4.2 No examples of data processing or data sharing with no contract or data sharing agreement respectively in place were identified through health checks.

4.3 As part of its ongoing work on transition of data protection artefacts from Programme to Social Security Scotland, the Data Protection Team has reviewed and where necessary updated data protection content in contracts which support delivery of transitioning products.

5. Data Subject Rights

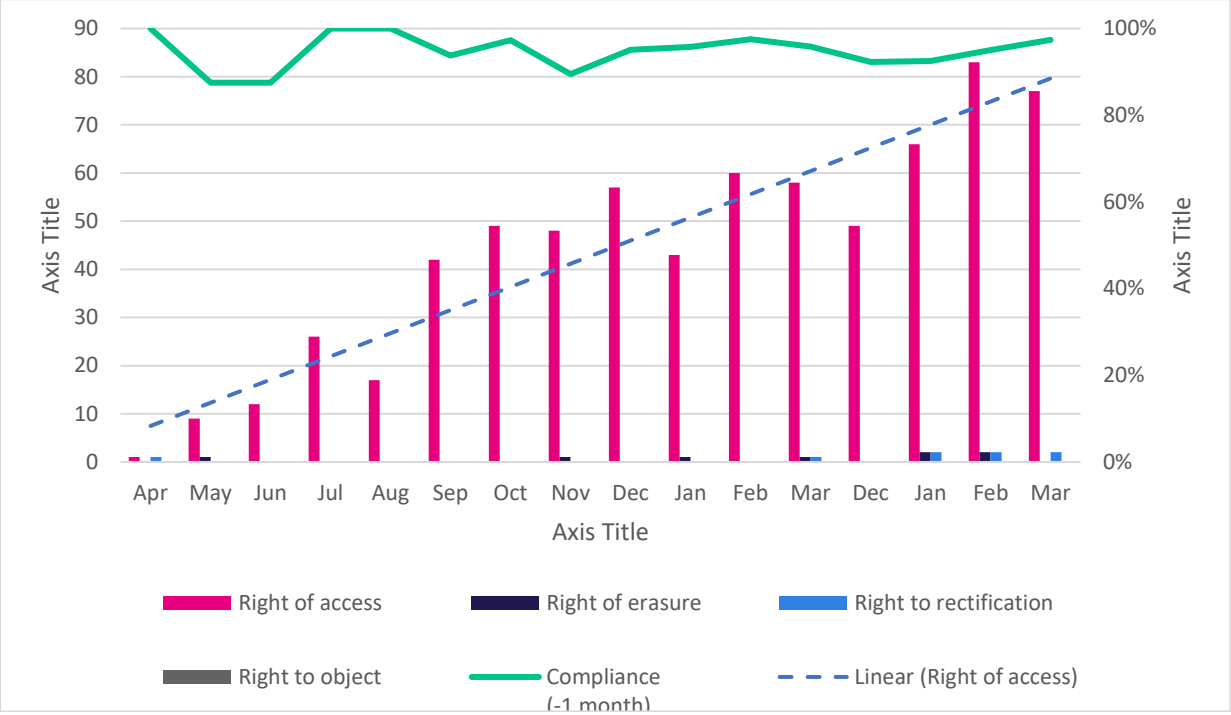
5.1 Social Security Scotland's requirement to notify data subjects of their rights under data protection legislation is delivered through privacy notices. The client-facing privacy notice was updated in November 2023. The privacy notice on the Social Security Scotland website was updated in August 2023. The employee privacy notice remains the responsibility of People Directorate in core Scottish Government. It is anticipated that this will be updated as part of the move to Oracle Cloud.

5.2 The Information Rights Team processed 527 data subject requests in 2023-24 up from 57 on the previous reporting year. This 909% increase is likely down to the organisation dealing with more complex disability benefits. This is also an indication that the awareness activities conducted during last reporting year has been successful and that staff are better able to recognise requests and direct them to the Information Rights Team.

5.3 The rate of increase in data subject requests appears linked with adverse decisions or delays in decision-making in disability benefits. Deficiencies in 'business as usual' processes, such as the ability to print and send a letter confirming benefits received by clients, lead to requests of this nature being treated as Subject Access Requests.

5.4 Most requests were for access with nine requests exercising other rights. The vast majority of requests were met within the prescribed period of one calendar month from date of receipt (see Figure 2). Dips in compliance have largely been caused by resourcing issues within the Information Rights Team. Difficulties remain in identifying and extracting clients' data from SPM, telephone recordings and webchats. Personal data relating to clients being stored outside SPM may risk compliance if volumes continue to increase.

Figure 2: Data Subject Requests 2023-24: Categories and Compliance Rate



6. Personal data breaches

6.1 The Data Protection Team investigated 1593 reported personal data incidents, of which 681 were assessed as actual personal data breaches. This represents an increase in breaches of 105% on 2022-23. The increase may be attributed to the increased volume of client transactions and new benefit types. Activity undertaken to promote colleagues' responsibilities for reporting potential breaches may also have contributed to an increase in reports through greater awareness.

6.2 Each reported personal data incident was assessed to determine the severity of the breach, analyse the root cause, and provide advice on mitigating any impacts on individuals and on preventing recurrence. Investigation of incidents often produces useful learning for wider application across the organisation (for example, training and development needs of colleagues other than those directly involved in an incident, system and process design), but this source of knowledge is underexploited. For example, the introduction of functionality in SPM to prompt client advisers to consider aspects of client address changes was designed and implemented without engaging the data protection team, and the functionality does

not therefore address all root causes of breaches, and has in fact contributed to creation of further breaches.

6.3 Incidents and breaches have a range of impacts on the individuals affected, ranging from:

- stress and worry (for example concerns over privacy if correspondence is opened by residents at a client's former address);

- financial hardship (if an application form is sent to an incorrect address, leading to a client not being able to apply for and receive a benefit); or

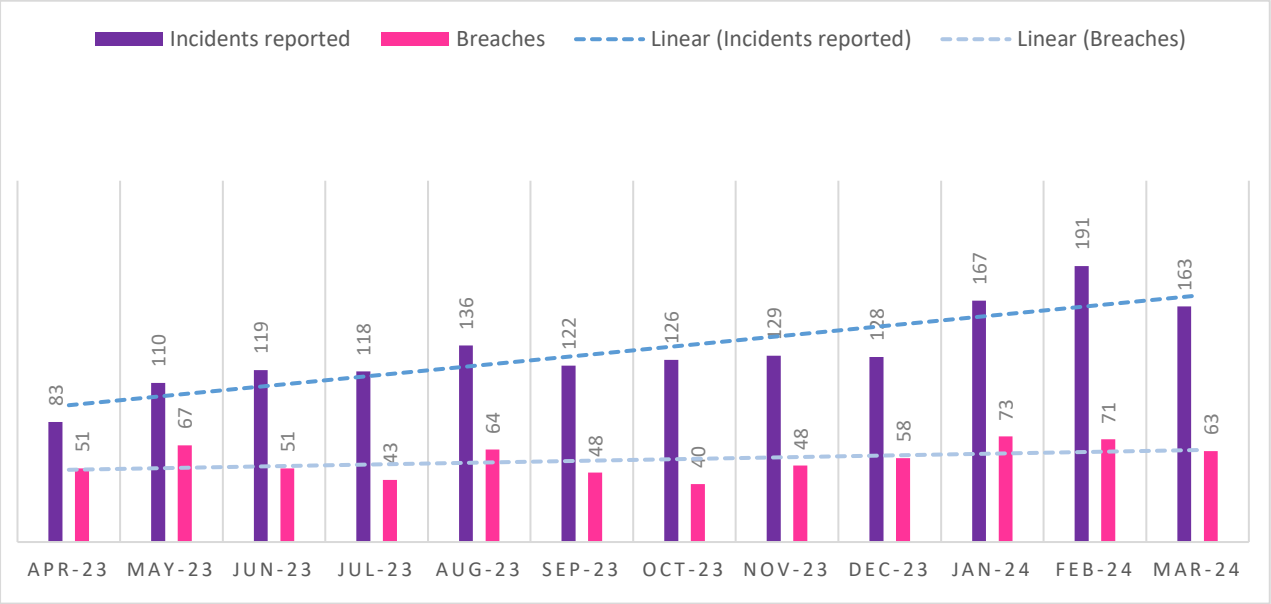
- fear of consequences (for example, if correspondence is sent to a previous address a client has left for domestic abuse reasons).

6.4 In all cases, breaches of clients' personal data is poor service and breaches of colleagues' data risks trust in the employer. Breaches pose a reputational issue, for example when a client or a member of the public reports an issue with correspondence being issued to an incorrect address, which can take client advisor time to resolve when the cause is not immediately apparent.

6.5 One breach was assessed as requiring notification to the Information Commissioner's Office (ICO) owing to the risks posed to the data subjects involved. The ICO made recommendations but took no further action in view of the action already taken by Social Security Scotland to minimise risk to affected subjects and lessons learned. This was the third time Social Security Scotland had been required to report such a breach.

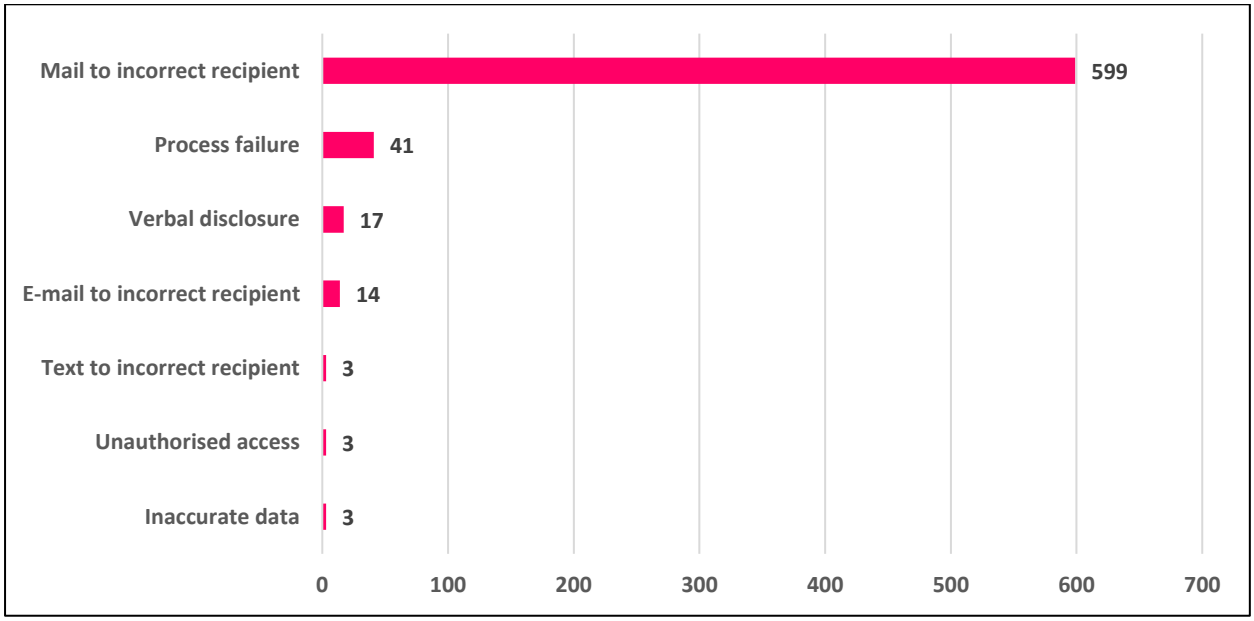
6.6 The proportion of system-generated breaches (i.e. breaches occurring when a system worked to design but where a process led to a personal data breach) compared to breaches caused by human error was 34% (33% in 2022-23).

Figure 3: Personal data incidents and breaches 2023-24



6.7 Figure 3 shows that suspected incidents are reported in greater and increasing numbers, while reported incidents identified as breaches are increasing at a lesser rate. This could be attributed to increased communications and engagement activities with colleagues. More staff are aware of when and how to report an incident, and are doing so. However, as overall knowledge and awareness of data protection increases, as a percentage of overall incidents, fewer incidents have been identified as breaches, when compared to 2022-23. This suggests good colleague awareness of procedures, along with a healthy culture of the need to report suspected breaches (reflecting awareness of the guidance on reporting breaches (see Figure 2 above).

Figure 4: Confirmed Breaches by Type 2023-24



6.8 A comparison with 2022-23 shows that breaches other than those categorised as “mail to incorrect recipient” (86 in 2022-23 and 83 in 2023-24) were stable, and were potentially fewer in 2023-24 than expected given a presumed correlation between the increasing volume of clients and the volume of breaches.

6.9 As can be seen from Figure 4, the overwhelming majority of breaches consist of mail being sent to an incorrect recipient. There are multiple causes for this, including:

- lack of client advisor awareness that when updating a client’s residential address that their correspondence address also needs to be updated where applicable;

- inadequate consideration in process design that holding two addresses for clients and a lack of robust measures to ensure both are accurate and up to date as necessary would be likely to lead to personal data incidents and breaches;

- inconsistent procedures across benefit types mean that not all client advisers are able to update correspondence addresses in the same way;

- inconsistent and incomplete and difficulties in updating Internal Knowledge Management hub guidance on change of circumstances across all benefit types;

- SPM design issues (correspondence addresses not created for clients applying with just a residential address, address change wizard not prompting consideration of change of correspondence address, relationships functionality changing addresses of clients inappropriately);

- data received from the Department for Work and Pensions containing out of date correspondence addresses over-writing up to date addresses already held in SPM;

- data received from the Department for Work and Pensions not indicating a correspondence address leading to the residential address being used for both inappropriately;

- change of circumstances tasks not being updated before correspondence is generated; or

- clients not updating Social Security Scotland of a change of address.

6.10 Reliance on letters as a key means of client communication, including letters containing special category data (for example Adult Disability Payment award letters), while factors above are at play risks repetition of these incidents and breaches and continued adverse impact on clients. Further system and process development should take these findings into account to design out vulnerabilities.

6.11 Inaccuracy of address information can also lead to impacts on wider organisational performance issues. For example, equality information not being gathered as a result of forms being sent to an inaccurate address could impact on our analytical reports. Errors with correspondence will lead to increases in processing times for the affected clients.

6.12 The root causes of these breaches are well understood, but remain unaddressed strategically by the organisation. Using intelligence and approaches developed through analysis of breach investigations carried out by the team, a personal data breach minimisation strategy was developed by the Data Protection Team and approved by the Information Governance Group in December 2023.

6.13 The strategy sets out information and analysis on personal data breaches and suspected incidents in the organisation, and a set of actions which the team will coordinate throughout 2024-25 to seek a reduction in personal data breaches and therefore impact on affected data subjects (clients, colleagues, and others).

Annex 1

Data Protection Assurance Health Checks

Ref No.	Business Area	Status
DPHC 01/21	**Mailroom (Pilot)**	Complete
DPHC 02/21	**Operational Finance**	Complete
DPHC 03/21	**Local Delivery (West)**	Complete
DPHC 04/21	**Resourcing**	Complete
DPHC 05/21	**Client Experience**	Complete
DPHC 06/21	**Low Income Benefits (Young Carer Grant and Job Start Payment)**	Complete
DPHC 01/22	**Low Income Benefits (Funeral Support Payment)**	Complete
DPHC 03/22	**Onboarding Team**	Complete
DPHC 04/22	**Debt Management**	Complete
DPHC 05/22	**External Investigations**	Complete
DPHC 06/22	**People Policy Advice & Wellbeing**	Complete

DPHC 01/23	**Child Disability Payment (Health & Social Care)**	Complete
DPHC 02/23	**Child Disability Payment (Client Services Delivery Processing)**	Complete
DPHC 03/23	**Child Disability Payment (Client Services Delivery Case Transfers)**	Complete
DPHC 04/23	**Child Disability Payment (Local Delivery- Case Advisors)**	Complete
DPHC 05/23	**Child Disability Payment (Local Delivery- Booking Team)**	Complete
DPHC 06/23	**Child Disability Payment (Quality Team)**	Complete
DPHC Review 01/23	**Payment Resolutions (Operational Finance)**	Complete
DPHC Review 02/23	**Resourcing**	Complete
DPHC 07/23	**Pre-employment Team**	Complete
DPHC 08/23	**Health and Safety Team**	Complete
DPHC 09/23	**Place Services**	Complete
DPHC 01/24	**Internal Investigations**	In progress
DPHC 02/24	**Adult Disability Payment (Client Services Delivery)**	Planned
DPHC 03/24	**Adult Disability Payment (Health and Social Care)**	Planned
DPHC 04/24	**Safeguarding**	Planned
DPHC Review 01/24	**Client Experience**	In progress
DPHC Review 02/24	**Mailroom**	In progress
DPHC Review 03/24	**Low Income Benefits (Young Carer Grant and Job Start Payment)**	In progress