



## POST OFFICE LIMITED

### AUDIT, RISK & COMPLIANCE COMMITTEE REPORT

---

<b>Title:</b>	Compliance and Audit Report	<b>Meeting Date:</b>	26 January 2021
<b>Author:</b>	Jonathan Hill, Director, Compliance Johann Appel, Head of Internal Audit	<b>Sponsor:</b>	Al Cameron, Group Chief Finance Officer Ben Foat, Group General Counsel

#### Input Sought: Noting

The Committee is asked to:

1. note the Compliance update, in particular:
  - The Controls Framework update;
  - The Data Management activities;
  - Post Office's approach to cookies;
2. note the Internal Audit update, specifically progress being made with delivery of the Internal Audit programme and completion of audit actions.

#### Previous Governance Oversight

Risk & Compliance Committee (RCC) on 12 January 2021

#### Executive Summary

This paper provides an update on key and emerging risks, compliance matters and an update on the latest internal audit position.

## Compliance

### Controls Framework

1. The Controls Framework project has been established, initially, to review/identify gaps in the controls established for the activities done to address the Group Litigation Order (GLO) matters. We are working with the Historical Matters Unit (HMU) project teams, who are identifying processes that have been updated or need updating following the Common Issues judgement (CIJ), Horizon Issues judgement (HIJ) and the establishment of the Stamps Scheme.
2. An interim report is expected from KPMG relating to the HIJ, which the Controls project will use as the basis to conduct controls reviews of the Horizon issues.

#### Progress to date:

3. Recruitment of experienced Controls Compliance Analysts.
4. The HMU team is mapping the processes and controls for Transaction Corrections, these are being reviewed by the Control Framework analysts.
5. Changes to around 70% of processes have been made to the Onboarding of new Postmasters, the Controls Framework project team is reviewing these to understand what controls are in place and how effective they are
6. Designing and building a temporary Workflow on 'Power Apps' Tool to record controls information against each business process, and facilitate assessment, assurance and MI for the Controls Framework project
7. Testing the workflow tool and producing a training pack for the business outlining how control owners and operators will need to support the project
8. Drafting a controls assurance template to support and facilitate the control assurance work, ensuring design and operating effectiveness and consistency of Controls work;
9. A review of the existing Operations processes and controls is underway working with the Ops teams, with a target completion of the start of February
10. A review of the Stamps stock, including controls is underway, aiming to complete in February 2021, subject to Covid restrictions.

#### Key issues:

11. Initial controls reviews have identified that there is no consistent approach to mapping the processes, and in some cases no maps, for activities addressing the CIJ remediation actions, which makes it difficult for the business to identify its controls and the project to provide assurance that the controls exist and are effective.

#### Remediation activities:

12. Where process maps are missing we are working with the HMU CIJ team to support the creation of process maps
13. This may lead to re-work to assess the robustness of controls, where additional activities are identified at a later date

#### Next steps:

14. Framework workstream:
  - Design business-wide controls framework (draft early January 2021)
  - Framework to be reviewed by external party (e.g., Deloitte) to ensure meets industry standards
15. Controls system
  - Define the user requirements for a permanent controls system (draft early January 2021)
16. CIJ controls review
  - Complete Operations controls review



- Refresh work plan following updated activity project plan from HMU team
- 17. HIJ controls review
  - Develop workplan following receipt of KPMG's HIJ interim review (early January 2021)
- 18. Stamps Stock review
  - Complete review of Stamps Stock actions, including associated controls (January-February 2021)
- 19. Business case
  - Develop business case for plus roll out of Controls Framework and Controls Framework system across all Post Office activities and functions

## Telecoms

### Sale

At the time of writing, the telecoms sale is due to complete in January 2021. A number of questions are still be addressed by the transaction team. These include:

- Management of historical and post-sale complaints relating to pre-sale matters.
  - The continuing of a PSD2 audit for premium rates calls, scheduled for January 2021.
  - Existing Ofcom information requests that are due in Q4 2020/21.
20. Ofcom has not yet been informed of the final decision but we have advised the Telecoms team this should be done ahead of signature.

### Comms incident

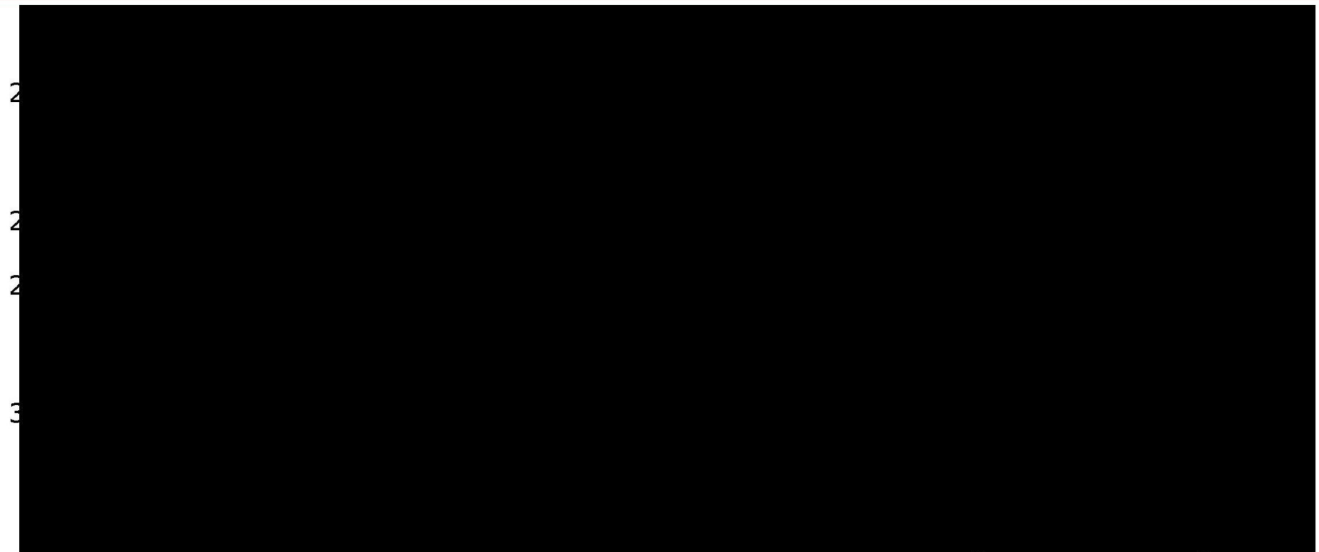
21. We are due to send Ofcom a letter to inform them that all inbound comms and outbound comms have been addressed to put the customer back into the circumstances they would have been if there had not been a communication failure. We are waiting to hear if Ofcom will investigate.

### Annual Best Tariff Notifications

22. Annual Best Tariff reminders have started being sent and are planned to be completed by 14<sup>th</sup> February 2021 in line with the regulation. We expect complaints to rise as customers will ask why they have been paying higher out of contract prices. Customers who have not been subject to a fixed commitment period will receive a bill message, Ofcom may consider that we should be more direct.

### Voice only customers

23. Ofcom has released the consultation on its approach to the voice only market, if Post Office were to remain in the telecoms business this would have a material impact on our ability to compete. Given the potential sale, Post Office is not responding to the consultation.
24. The Telco regulatory developments are highlighted at Appendix 1.



CCRC, PCDE and HSS

31. The 4 November Historical Matters Steering Committee approved the recommended actions with these to be undertaken on an expedited basis, having regard to the 5 February 2021 deadline date for disclosure for the 41 past convictions referred for appeal by the CCRC to the Court of Appeal (Criminal Division).
32. Peters & Peters (P&P) has now applied, in conjunction with Herbert Smith Freehills (HSF), case specific and non-case specific search terms to the indices to identify material that may be relevant to the PCDE. The searches resulted a number of records (files or boxes) that have been categorised as either
  - Potentially relevant records (e.g. because the descriptions are vague but they contain relevant words, or they are relevant but the date is outside the relevant review period)
  - relevant to the PCDE and malicious prosecution workstream based on the descriptions in the indexes.
  - Records that are not relevant
33. The 10 December Historical Matters Decision Forum approved a recommendation from P&P to
  - Request all of the clearly relevant records for physical checking
  - Complete a sample of the potentially relevant records. This review is nearing completion and relevant documents were identified in c10% of the boxes sampled. P&P are considering if more records need to be checked. The relevant records identified included
    - case specific material relevant to an individual prosecuted by Post Office Limited (POL)
    - documents where an acquitted individual raised issues with Horizon
    - documents relating to issues identified during the roll-out of Horizon, or shortly before
    - prepared statements for interview
34. The wider "dip sample" exercise of a statistically representative random group of indexed and unindexed boxes (c.100 of each) is being progressed by HSF.
35. The records that form the sample have been retrieved. The scanning was initially delayed due document quality but it is now progressing.
36. In parallel, the HSF case handlers have been trained, enabling the reviews to start w/c 7 December. The sampling is due to complete w/c 25<sup>th</sup> January.

37. The outcome of the reviews will be reviewed throughout the sampling exercise to give early indication of any potential follow up action. The initial feedback indicates that a significant proportion of the records are receipts. Work is in progress to understand the potential relevance of receipts to the PCDE and HSS activity

Back office sites record assurance review:

38. The RCC instructed Compliance and Legal to instigate a search of all Post Office back office locations to give assurances that all relevant information has been presented to Counsel for Starling and PCDE purposes.
39. 93 locations were initially identified as being in scope.
- 44 were de-scoped as they have been determined to be 'vacant'
  - Vacant premises had to be cleared of all materials including records.
40. All location searches have been completed and results collated. Of all sites searched there are five deemed potentially to be of relevance;
- Swindon – a high number of sealed packages may be of relevance these were being checked, under external counsel guidance, on 15<sup>th</sup> January for materiality. Plans are in place to move these to P&P should they be needed.
  - Chesterfield – P&P had already visited Chesterfield and retrieved all materials that appeared relevant. However, the number of records identified by this latest search (c.2,300) was significantly higher than expected. Plans are in place to verify numbers and run checks on any additional new records, which should be completed by 18<sup>th</sup> January.
  - Bolton – 15 boxes of transactional records have been located and currently being investigated under guidance from P&P. Any in-scope documentation will be sent direct to P&P.
  - Swansea – All relevant files are being collected on 18<sup>th</sup> January for delivery to P&P.
  - Mutley (Plymouth) - Full mail sacks from branches have been stored there over the years. These are being checked, guidance from P&P. This will be completed by 18<sup>th</sup> January.
41. The Legal and search teams are confident that the necessary searches will be complete for 5<sup>th</sup> February deadline for PCDE purposes

Record retention

42. The RCC Data Management paper identified that Post Office businesses needed to give assurances that Record Retention Schedules, agreed as part of the Record Retention Programme, were accurate and covered all processing activities.
43. All Data Owners were identified and provided with a copy of the Retention Schedules, Remediation Logs and copies of the Document Retention and Disposal and Protecting Personal Data policies.
44. Data Owners have expressed concerns with regards to the implementation of the Remediation requirements. The key barriers reported back so far have been lack of resource to implement the changes and the timeframes set for remediation to be complete.
45. The responses from the data owners are being recorded and consolidated by the Chief Information Security Officer (CISO) team as the owner of the record retention policy and compliance is supporting the team. Going forward this should be coordinated through the Data Governance framework.

Record management in branches

46. Compliance, Property Services and the Network team have stood up a project to implement a change programme for Records Management with the Branches. This project will look to:





- Identify and communicate out to Branches what information needs to be archived and preserved
  - Create a new process for record archiving on a regular basis and not just on the closure of a branch as is the process today
  - Arrange for the necessary materials to be provided to branches to allow for archiving to occur, including boxes, archive content labels and deletion dates
  - Mechanisms for transferring boxes of records from branches to off-site storage facilities.
47. The key challenges will be ensuring that;
- this project is sufficiently resourced to allow the new processes to be implemented,
  - New processes are developed and shared with relevant stakeholders for consultation
  - Communications and training materials created and shared across the Network to enable a smooth transition into Business as Usual.
48. This work will commence in early 2021 as resources were focussed delivering Christmas in branches and on the searches of back office locations.

#### Post Office Ltd approach to Cookies:

49. The CNIL (French Data Protection regulator) levied significant fines of €100m and €35m respectively against Google (US parent organisation and Ireland subsidiary) and Amazon Europe for breaching French Data Protection legislation with regards to their use of website cookies under the ePrivacy directive. The ruling is not applicable in the UK. However, the ICO is likely take into consideration the finding of the CNIL.
- Google – CNIL were clear that cookies are only lawful if informed consent has been given. Consent should be requested using a banner on the user's first site visit with a clear link to how cookies can be disabled or opposed. Ability to refuse should be offered in whole and part with information disaggregated by purpose. CNIL imposed a deadline of 3 months to ensure individuals were adequately informed otherwise a further penalty of €100k would be imposed for each day of delay.
50. Post Office continues to be 'middle of the pack.' We believe the Google ruling may have an indirect bearing on our approach to cookies. Therefore, the Digital team and Compliance is assessing the implications of the ruling and possible changes to our Cookies approach. Changes could include:
- Default settings for all cookies except necessary to be switched to 'off' in preference centre
  - Persistent bookmark on all pages of Post Office website to allow users to re-access the preference centre at any time
  - Detailed information provided through cookie policy on vendors and duration

#### General Data Protection Regulation (GDPR) Contract Remediation

51. The Contract Remediation project was formally closed at the end of July as reported to the previous RCC. Work is ongoing on and the number of outstanding contracts is 5, 2 fewer than reported at the previous Committee meeting.
52. Fujitsu has agreed all GDPR clauses in the main contract. The only outstanding issue is with one processing schedule, which requires Legal to agree a position on.
53. We have received a response from Fujitsu Telecoms (FJT). FJT's response is disappointing given the number of changes it has proposed and that are non-GDPR compliant. The Telecoms team, together with Legal and Compliance, is working to close this down quickly as it is required to conclude the overall sale agreement.
54. Monthly Contract Review Group meetings continue to monitor progress and support negotiations. This will continue until all outstanding contracts are finalised.



## Financial Crime

### Compliance with Money Laundering Regulations

55. Please see the separate annual Money Laundering Reporting Officer (MRLO) report.

### Anti-Bribery and Corruption ("ABC") update

56. Overall completion of the annual ABC training was 98.4% as at 15<sup>th</sup> December 2020. The business unit previously at 81.7%, is now at 92.4% completion rate and Learning & Development are liaising with HR Business Partners to identify better controls for contractors.

57. Submissions on the gifts and hospitality tool remain low due to Covid restrictions, however a reminder was issued to colleagues in November due to a potential increase in gifts leading up to Christmas.

### Whistleblowing Update

58. All reports received in the last two months relate to the branch network, with the majority received from agent assistants raising concerns about Postmasters and unethical behaviour or conduct. Two reports received relating to a Postmaster subsequently uncovered potential mails fraud that is estimated to be in the region of £500k. This is currently being investigated by Post Office Security Operations, supported by the Royal Mail Investigations team.

59. The contract to procure Protect (UK Whistleblowing Charity) to enable us to undertake self-assessment and benchmarking is nearing completion and this should commence in January. Protect have been asked to deliver tailored training for GE and Senior Managers as early as possible in 2021 and we are awaiting their proposals.

### Fit & Proper update

60. Please see the separate annual Money Laundering Reporting Officer (MRLO) report.

### External Threats

61. Please see the separate annual Money Laundering Reporting Officer (MRLO) report.

### Supply Chain Compliance

62. Remote audit of Supply Chain is progressing, and an interim update has been provided to Supply Chain outlining seven key findings identified to date, to enable them to commence mitigation. Some potential issues have been highlighted relating to outstanding actions in respect of fire risk assessments undertaken in June and July which are currently being investigated by the Head of Health & Safety. It is anticipated the audit will conclude by the end of December.

## Financial Services

### Multi Principal Review of 1<sup>st</sup> line controls.

63. Our three regulatory principals, Capital One, Bank of Ireland (BoI) and Post Office Management Services Limited (POMS), are reviewing mystery shopping, training, the risk management framework, quality of sales oversight and internal governance as part of their oversight of the Post Office.

64. The discovery work has recently completed and whilst there will be areas of improvement highlighted, there do not appear to be any material issues raised that would cause the Principals to alter their selling/introducing regulated activity with the Post Office.

65. Whilst we are supportive of this review there a number of items in a 'statement of facts' document that need to be clarified before a draft report is produced.

66. We expect the final report to be produced late January and we will share this with this Committee.





---

### Compliance Monitoring

- 67. Following the implementation of the latest Covid-19 lockdown, with the agreement of our Principals, mystery shopping was suspended. This will be reviewed when conditions allow.
- 68. Sales of Travel Insurance are currently suspended in branch; all of our other financial services products remain on sale and promotional activity is planned for both protection and savings business. As with previous lockdowns, we will focus on remote monitoring measures to review performance such as cancelations, complaints and customer validation calls and regular governance meetings with the Principals remain in place.

### FS Key Regulatory updates

- 69. A summary slide of the key future developments is included in the reading room at Appendix 2.
- 70. Post Office responded to the Her Majesty's Treasury (HMT) call for evidence on Access to Cash in November, which sets out the government's aims for protecting access to cash throughout the UK. Post Office outlined the well-established and increasingly important role it plays in access to cash.
- 71. As part of this consultation the government is considering imposing a single regulator to have responsibility for a well-functioning cash retail distribution network. We await the government response (no date has been given for this) but we will need to understand any potential regulatory risks or implications for Post Office if it is decided that the cash infrastructure should be regulated.
- 72. The Financial Conduct Authority (FCA) has withdrawn its proposal to establish a single easy access savings rate for all savings account of over one year. This is welcome as it could have caused significant challenges for the future pricing of savings back books and the need to change systems with our partner BoI.
- 73. The Overall Compliance Dashboards (Appendices 3 and 4) are included in the reading room.

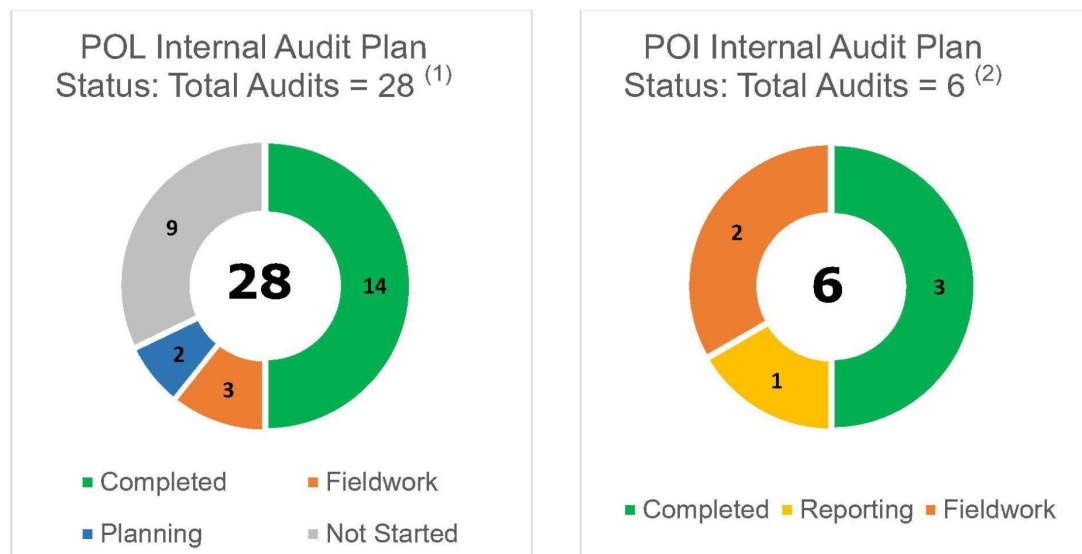




## Internal Audit

### Progress against Internal Audit plan

74. Delivery of the 2020/21 programme is making good progress, with a further five audits completed since the November ARC meeting (4 POL & 1 Post Office Insurance (POI)). In addition we have also issued one interim report on the Historic Matters CIJ Improvement Programme.
75. Current delivery status is as follows:



<sup>(1)</sup>Target number of reviews based on revised plan for 2020/21 approved by ARC (18 Internal control reviews & 10 change assurance reviews). Details of the audit plan status are included in the reading room (Appendix 10).

<sup>(2)</sup>POI ARC approved baseline plan for 2020/21.

76. A re-prioritised Internal Audit programme was approved at the May ARC meeting in response to Covid-19. A more dynamic (quarterly rolling) audit plan was adopted and is being reviewed at each ARC. Further revisions to the plan was approved at the September ARC meeting and is included in the reading room (Appendix 10).

77. The following audits are planned for delivery in Q4:

	Review	Sponsor	Timing	Status
1	Historic Matters (Post GLO) Set-up and Governance	Declan Salter	Oct	Fieldwork (Interim Report Issued)
2	Historic Matters - CIJ Operations Improvement Programme	Declan Salter	Nov	Fieldwork (Interim Report Issued)
3	Postmaster Reporting (MI, Branch Trading Statements)	Amanda Jones	Jan	Fieldwork
4	Postmaster Remuneration (3 <sup>rd</sup> Party Data)	Amanda Jones	Feb	Planning
5	Historic Matters - HIJ Operations Improvement Programme	Declan Salter	Feb	Not Started
6	GLO Historical Shortfall Scheme – Claims & Payments	Declan Salter	Mar	Not Started
7	Third Party Revenue Data Assurance	Al Cameron	Feb	Planning
8	Change Controls Effectiveness	Dan Zinner	Feb	Not Started
9	Strategic Platform Modernisation	Jeff Smyth	Mar	Not Started




## Internal Audit reviews completed

78. The following POL audits were completed since the November ARC meeting:

1	IT Control Framework		4	Belfast Exit Follow-up (Programme Assurance)	
2	Mails & Parcels		5	PCI Compliance (Programme Assurance)	
3	Historic Matters – CIJ Operations Improvement Programme (Interim)				

79. Our findings and observations from these reports are summarised below (par. 80-84), with the full reports available in the reading room (appendices 5-9).

### 80. IT Control Framework (Ref.2020/21-13)

 <p>Needs Improvement</p> <p><b>Sponsor:</b> Jeff Smyth</p> <p>Audit actions:</p> <table border="1" data-bbox="203 1056 397 1203"> <tr> <td>P1</td><td>0</td></tr> <tr> <td>P2</td><td>5</td></tr> <tr> <td>P3</td><td>2</td></tr> <tr> <td>Total</td><td>7</td></tr> </table> <p>Appendix 5</p>	P1	0	P2	5	P3	2	Total	7	<p>The purpose of the audit was to assess how effectively the IT Control Framework (ITCF) supports IT control assurance and risk mitigation for POL, and whether it reflects the operation of IT related controls across the business and provides accurate and timely information on control performance.</p> <p>We believe that the approach to implementing the ITCF is sound, based on alignment with an internationally recognised governance framework, with quarterly self-assessment and monthly reporting of status and remediations. The 268 controls that make up the ITCF and are largely aligned with what's happening on the ground and the self-assessment process was generally operating effectively.</p> <p>Additional work is required to ensure that the ITCF fully supports the business. This should be addressed through migration to a more comprehensive risk and control management tool, and the introduction of strong second line activity to independently validate the self-assessment process.</p> <p>We conclude that the ITCF has continued to mature since its implementation in 2018 and has further improved since our previous review in 2019. However, we highlight that the operation of the ITCF is not yet fully embedded within the business and was impacted by the absence of a key staff member during April to July 2020.</p>
P1	0								
P2	5								
P3	2								
Total	7								
<p><u>Management Comment provided by Tony Jowett (CISO)</u></p> <p>"Our IT controls framework allows us to better mitigate risks impacting POL's IT. We have reached a very good basic standard of maturity against COBIT 5 and other controls frameworks. This report comes at a perfect time to help us move to the next level of controls maturity. I accept the findings in it and will work to address them. Many thanks for the input."</p>									



## 81. Mails & Parcels (Ref.2020/21-16)



Needs Improvement

### **Sponsor:**

Owen Woodley

### **Audit actions:**

P1	1
P2	4
P3	0
<b>Total</b>	<b>5</b>

Appendix 6

The Mails & Parcels business is of key strategic importance to Post Office, contributing one third of PO's total revenue (approximately £350m) in FY20. In Q3 FY21 Mails & Parcels contributed 63% of all Network income.

The purpose of this audit was to review both the Customer and Postmaster journeys for Mails and Parcels products, and to assess the controls in place over related financial, operational and compliance processes.

We found that Post Office are maintaining a positive and effective relationship with Royal Mail Group (RMG), having just successfully negotiated and signed a new 11 year agreement (MDA2).

However, the audit highlighted several issues concerning worsening performance with respect to compliance with Prohibited and Restricted Items (Dangerous Goods) requirements. Segregation of parcels and accuracy of Mail Redirection forms were similarly underperforming, both of which have resulted in significant Service Credits being applied by RMG in FY20 and are expected to recur for FY21.

There are currently limited consequences at branch level for underperformance and non-compliance in these areas. If performance in these areas are not improved, the level of Service Credits being applied by RMG will increase when the new Mails Distribution Agreement (MDA2) comes into effect.

### Management Comment provided by Tom Wasilewski (Head of Commercial Development)

"Given the growing importance of Mails to both the Post Office and our Postmasters a thorough review and audit of its key processes is crucial. The areas highlighted for improvement are right focusing on important drivers of safety and financial performance, and it is satisfying, given the recent signing of the new agreement with RM, that no issues were identified in how that relationship is managed. Compliance and enforcement of Prohibited and Restricted Items (Dangerous Goods) is critical to delivering the high levels of mails integrity our customers expect and the downward trend is concerning making an urgent focus on improvement a priority. However, given the multiplicity of causes and the scale of the network, it is a challenge for which the Mails team will need support from colleagues across the business and we look forward to working closely with them in turning this around. The improving trend in segregation is encouraging and the new contractual arrangements under MDA2 make achieving the new target across all areas a priority".

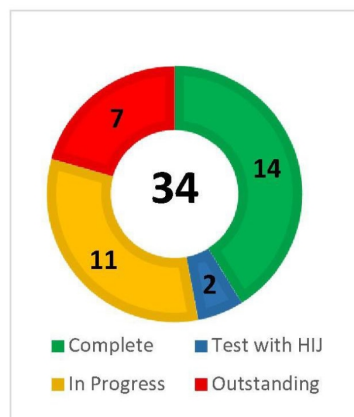




## 82. Historic Matters – CIJ Operations Improvement Programme (Interim Report) (Ref.2020/21-15)

### **Not Rated** (Interim Report)

Progress with completion of NRF recommendations:



**Sponsor:**  
*Declan Salter*

Management comments and audit actions will be in the final report.

*Appendix 7*

Following the judgments from the Group Litigation Order, Post Office has undertaken a programme of improvements to overhaul culture, practices and procedures throughout every part of the business. In addition to launching the Historical Shortfall and Stamps Schemes, as part of its operational improvement plan, and to address issues which arose from group litigation concluded last year, Post Office has established a new Historic Matters business unit (HM) to oversee and deliver the programme of improvements.

Internal Audit is performing a review of the management and oversight of the improvements delivery, as well as, the appropriateness and sustainability of plans to address the Common Issues Judgment (CIJ) and Horizon Issues Judgment (HIJ) findings. This is being done in three phases.

This second phase of the audit work assessed the programme of measures that will oversee the delivery of the operational improvements to address the criticisms from the CIJ. Primarily, we sought to gain assurance that the operational improvements recommended by Norton Rose Fullbright (NRF), as a result of their analysis of the judgment, have been identified and implemented in accordance with the planned timescales.

We concluded that considerable work has been done to address the judgment findings and implement the 34 NRF recommendations. The status of completion of the recommendations at the time of the audit report, is shown in the chart to the left.

Progress is well evidenced throughout, although in some instances, we have noted differences between the project's view of progress, compared to that of Operations. There is an opportunity to address this by the adoption of a formal handover process that clearly assigns the acceptance of amended documents and procedures by BAU operations.

We highlight that further activity will be required within the business to absorb the impact of the recent OE and the premature departure of some key senior colleagues.

Management Comment provided by Amanda Jones (Retail and Franchise Network Director)

"There has been progress on the remedial actions on the NRF report and we expect to have the majority of actions completed by the end of February with a clear plan to completion for any that may remain open. The change in ownership has enabled further multiple reviews of our responses (including by the HMU) to NRF's recommendations and our aim, where possible, is to go beyond legal compliance to make appropriate operational and cultural improvements to our processes. All actions are tracked with weekly reporting to GE."



### 83. Belfast Exit Follow-up (Programme Assurance) (Ref.2020/21-11)



Needs Improvement

**Sponsor:**  
Jeff Smyth

Audit actions:

P1	0
P2	3
P3	4
Total	7

Appendix 8

Belfast Exit, also known as 'Pivot 2 Cloud', aims to migrate Horizon - the combined group of applications that supports the Retail business of Post Office - from the Belfast data centres (managed by Fujitsu) onto a new cloud platform. The programme was last assessed by IA as part of the 2018/19 plan, with a follow-up review agreed as part of Internal Audit's approved 2020/21 plan.

The objective of this follow-up review was to gain assurance that the revised programme set-up, governance and delivery processes are fit for purpose and operating effectively to enable the envisioned benefits of migrating to the cloud.

Since its restart, the programme has focused on ways to reduce complexity, add scale and delivery throughput, seeking opportunities to add contingency and reduce delivery risks. However, despite the good work done by the team, the technical challenges and the risk of in-flight delays remain significant, as is the potential future cost of failing to address some of the technical challenges faced (technical debt), in order to focus on optimising delivery.

We have rated the programme delivery as Needs Improvement, however, we highlight that **there is a significant residual risk that is outside of the control of the programme**. This risk relates to the fixed deadline of exiting the datacentre when the current lease expires. Management is currently assessing contingency arrangements, with the most likely scenario being a lease extension at an approximate additional cost of £4m. As a result, benefits originally forecasted for FY22 and FY23 may not be achieved.

We also highlight that the Belfast Exit and PCI Compliance programmes both share a heavy reliance on Fujitsu subject matter experts and a single test environment, thus competing for the same resources.

#### Management Comment provided by Rob Wilkins (Cloud Services Director)

"Good progress has been made with the 1<sup>st</sup> application migrated within 4 months of restart, a significant improvement on previous attempts to migrate and the introduction of AWS to assist in the planning and approach has yielded improvement. However, the success of the programme ultimately sits with Fujitsu given their intrinsic knowledge of the Horizon application. There are significant constraints placed on the delivery team, namely the lack of Fujitsu technical subject matter experts who understand Horizon, and only a single functional test environment. Both of these constraints are in contention with PCI and other projects and programmes. There are also significant interdependencies between this programme and PCI that need to be tightly managed, one can and will impact the other if they are independently unable to keep to schedule. In order to mitigate the risk of programme overrunning, POL is working with Fujitsu's facilities team to secure short term lease extensions. The team need to also understand the potential that COVID restrictions/impacts could have a knock-on effect on its ability to maintain schedule given the significant amount of technical change the programme introduces."





#### 84. PCI Compliance (Programme Assurance) (Ref.2020/21-17)



Needs Improvement

**Sponsor:**  
Jeff Smyth

Audit actions:

P1	0
P2	2
P3	1
Total	3

Appendix 9

The PCI compliance programme is a key compliance risk mitigation programme for Post Office with a high level of risk, complexity and cost. The implications and the level of changes needed to processes and systems supporting both Payment and Banking Services, have led to multiple programme iterations with several business case revisions.

The programme was last assessed by Internal Audit as part of the 2019/20 plan and a follow-up review agreed as part of Internal Audit's 2020/21 plan. The objective of this follow-up review was to gain assurance that the revised programme set-up, governance and delivery processes are fit for purpose and operating effectively.

Significant improvements have been made to the programme since the 2019/20 assessment. In addition, the degree of confidence over the programme's ability to deliver has increased, with the programme highlighting its underlying assumptions and risks in the recent funding submission.

Despite the good work done, key challenges remain in the delivery of a PCI compliant environment. This is primarily a consequence of the inherent complexity of the chosen solutions, which are partly bespoke and the heavy reliance on third parties.

There is a risk of additional costs and further delays in completing the programme, which is not completely within Post Office control, as the current delivery approach is governed by a Time and Materials (T&M) contract with Fujitsu (with Ingenico operating as a subcontractor of Fujitsu).

We note that the programme is still facing challenges in the level of transparency and ease of engagement at functional level with Fujitsu and Ingenico.

We also highlight that the Belfast Exit and PCI Compliance programmes both share a heavy reliance on Fujitsu subject matter experts and a single test environment, thus competing for the same resources.

#### Management Comment provided by Rob Wilkins (Cloud Services Director)

"A good document with some useful insights which while identify areas where improvement is needed also highlight how far the programme has come over the last 9-12months. The report references that POL are very reliant on its suppliers to deliver this along with other projects and programmes who are contending for the same resources. In order to ensure the best chance of a successful delivery of this programme, it has been prioritised at the expense of other initiatives which are contending for the same limited resources and test environment. That said, the programme has recently slipped twice due to other POL priorities (changes to support Brexit and RM contract changes) both of which had a 2 week impact to the schedule. The next 2 quarters are key for this programme as it looks to take the P2PE solution to full pilot and rollout, the latter could present significant challenge should the UK still be under COVID restrictions – this should be closely monitored."





## Post Office Insurance (POI) Audit Programme

85. The table below shows the status of the POI audit programme:

	Review	Timing	Status / Rating
1	Cyber Security (POL-POI Gap Analysis)	Aug	Satisfactory
2	Incident and Breach Management	Aug	Reporting <sup>N1</sup>
3	Data Governance: Ethics, security and privacy <ul style="list-style-type: none"> <li>Phase 1 – Third Party Data Security</li> <li>Phase 2 – Data Governance</li> </ul>	Sept Dec	Complete (interim report) Fieldwork
4	Special Investigation (Confidential)	Sept	Complete (not rated)
5	Pricing: Principles, policies and process	Nov	Complete, pending POI ARC submission
6	Financial Promotions Communications	Jan	Fieldwork
7	Effectiveness of Risk Management – original plan	Q4	Not started
8	Channel review: Non-branch sales – original plan	Q4	Being re-assessed

<sup>N1</sup> This audit was delayed due to special investigations undertaken at management request and with POI ARC approval.

## Status of Audit Actions

86. During May 2020 we agreed with management to provide extended completion dates for 14 actions impacted by Covid-19. All 14 actions have now been completed.

87. The movement and ageing of audit actions are shown in the table below (status at 18 January 2021).

Audit Action Status (POL):		Ageing:	
Open actions at last ARC	29	Open (not yet due)	34
Less: Actions closed in period	18	Overdue (<60 days)	1
Add: New actions in period	24	Overdue (>60 days)	0
Total open actions	35	Total open actions	35

88. Following is a summary of the one overdue action and latest status update:

Description of audit finding and Priority rating	GE owner and due date	Action Owners and Status Update
<b>Health &amp; Safety Response to Covid-19</b>		
<p><b>Finding (P2):</b> No formal collation and review of home working assessments undertaken.</p> <p><b>Action:</b> The Health and Safety team will work with HR to ensure that the appropriate assessments have been completed for all affected colleagues and the necessary actions taken to ensure safe working practices whilst working at home and, where appropriate, e.g. following an Occupational Health assessment adjustments supported and implemented.</p>	<p>Al Cameron</p> <p>Original date: 31/10/2020</p> <p>Revised date: 31/12/2020</p>	<p><b>Owner:</b> Martin Hopcroft</p> <p>It was decided to delay the process until after the busy Christmas period. GE PAs are currently collating a return on behalf of their lead teams to confirm that the activity has been completed. The H&amp;S team are offering support to any team who has questions or concerns. The team will be working around the PAs to undertake this check and collate the summaries during January. An update will be provided to the Safety Board on 27<sup>th</sup> January.</p>

---

## Appendices<sup>1</sup>

### Compliance

- Appendix 1: Telecoms Regulatory Calendar
- Appendix 2: FS Regulatory Calendar
- Appendix 3: Compliance Dashboard summary
- Appendix 4: Compliance Dashboard

### Internal Audit

- Appendix 5: Internal Audit Report – IT Control Framework
- Appendix 6: Internal Audit Report – Mails & Parcels
- Appendix 7: Internal Audit Report – Historic Matters – CIJ Improvement Programme
- Appendix 8: Internal Audit Report – Belfast Exit Follow-up (Programme Assurance)
- Appendix 9: Internal Audit Report – PCI Compliance (Programme Assurance)
- Appendix 10: Internal Audit Plan for 2020/21

---

<sup>1</sup> Appendices are accessible in the Diligent Reading Room.