



POST OFFICE LIMITED

Meeting:	Audit, Risk & Compliance Committee (ARC)
Date:	28 January 2020
Time:	09.30 - 12.00
Location:	1.19 Wakefield, Finsbury Dials, 20 Finsbury Street, London, EC2Y 9AQ

Present:	Other Attendees:
Carla Stent (Chair)	Jeff Smyth (Digital Technology Director, CIO FST & Identity): Item 4
Ken McCall (SID)	Rob Wilkins (Portfolio Director): Item 4
Tom Cooper (NED, UKGI)	Tony Jowett (Chief Information Security Officer): Items 4, 12.1
Zarin Patel (NED)	Andrew Goddard (Managing Director, Payzone): Item 5
	Mark Dixon (Head of Treasury, Tax & Insurance): Items 6, 7
Regular Attendees:	Dan Zinner (Chief Transformation Officer): Item 8
Tim Parker (Chairman, POL)	Sally Smith (MLRO): Item 9
Nick Read (CEO)	Tim Armit (Business Continuity Manager): Item 10
Alisdair Cameron (CFO)	Meredith Sharples (Director, Telecoms): Item 11.4
Ben Foat (General Counsel)	
Andrew Paynter (Audit Partner, PwC)	Observers:
Sarah Allen (Audit Senior Manager, PwC)	Rebecca Barker (Head of IT & Digital Risk)
Johann Appel (Head of Internal Audit)	Audrey Cahill (Risk Business Partner, Central Risk)
Mark Baldock (Head of Risk)	
Jonathan Hill (Compliance Director)	
David Parry (Senior Assistant Company Secretary)	

Time	Item	Owner	Action
09:30	1. <u>Welcome & Conflicts of Interest</u>	Chair	Noting
09:35	2. <u>Update from Subsidiaries:</u> Post Office Management Services (ARC)	Chair	Noting
09:40	3. <u>Previous Meetings</u>	Chair	
	3.1 Minutes: 25 November 2019		Approval
	3.2 Minutes: 25 November 2019 closed session		
	3.3 Action List		Noting & Input
	3.4 Draft Risk and Compliance Committee Minutes 14 January 2019		Noting
09:45	4. <u>PCI-DSS and Cyber Security Update</u>	Jeff Smyth	Discussion
	4.1 PCI-DSS – verbal update	Rob Wilkins	
	4.2 Cyber Security Update	Tony Jowett	
10:00	5. <u>Payzone Risk Report</u>	Andrew Goddard	Noting
10:15	6. <u>Tax Update and Annual Tax Strategy</u>	Mark Dixon	Noting, Approval
10:25	7. <u>Corporate Insurance Renewal</u>	Mark Dixon	Ratify



POST OFFICE LIMITED

10:30	8.	<u>Strategic Portfolio Office Change Control Environment Update</u>	Dan Zinner	Noting
10:40	9.	<u>Money Laundering Reporting Officer (MLRO) Annual Report</u>	Sally Smith	Noting
11:00	10.	<u>Business Continuity Update</u>	Tim Armit	Noting
11:10	11.	<u>Consolidated Report from Risk, Compliance and Internal Audit</u>		
11:10	11.1	Risk Report	Mark Baldock	Noting
11:20	11.2	Compliance Report	Jonathan Hill	Noting
11:30	11.3	Internal Audit Report	Johann Appel	Noting
11:40	11.4	PSD2 Implementation – verbal update	Meredith Sharples	Noting
11:50	12.	<u>Policies for Approval</u>		Approval
	12.1	Cyber and Information Security Policy	Tony Jowett	
11:55	13.	<u>Any other Business</u>	Chair	

Next ARC Meeting: Tuesday, 24 March 2020 at 09.00 to 11.30 in 1.19 Wakefield, Finsbury Dials, 20 Finsbury Street, London, EC2Y 9AQ



Post Office Limited Audit, Risk & Compliance Committee Report

Title:	Post Office Insurance ARC Update
Meeting Date:	28 January 2020
Author:	Ian Holloway, Director of Risk and Compliance, Post Office Insurance
Sponsor:	Amanda Bowe, POI ARC Chair

Input Sought

Action Required:	Noting
Previous Governance Oversight:	POI ARC November 2019

Executive Summary

Context:	<p>This paper provides a concise update on relevant POI matters for consideration by the POL ARC.</p> <p>The report is relatively short as Post Office Insurance (POI) ARC does not meet until 5 February 2020.</p> <p>A further update on anything material emerging from the February meeting will be provided in March 2020 to POL ARC.</p>
-----------------	--



Questions asked & addressed

1. What are the key points considered within the POI Risk and Compliance meeting which the POL Risk Committee should be aware of?
2. **Quality of sales improvement** - At the November ARC, a first line paper was presented on the quality of sales within the branch network. Whilst some improvements have been seen in overall sales quality as measured by videoed mystery shops, issues remain. These issues are often simple issues such as not discussing the wider POI protection product range or not asking smoking questions appropriately.
3. There is no evidence from downstream indicators such as complaints or claims declination that customers are achieving poor outcomes, but POI Management are clear that more work is required to achieve appropriate sales quality. POI are making term assurance sales introducer only and are withdrawing the Easylife product from branch sale. This leaves only travel and Over 50s life as branch based offerings. These changes will be complete by 31 January 2020. Both of these products sell relatively poorly in branch and the lack of sales volume inevitably contributes to overall quality issues. POI Management will also focus on enhancing training and working on a clearer channel strategy for the branch network. It will also look at the feasibility of directly controlling mystery shopping activity so it can better focus work on areas of greatest concern.
4. **Data breach** - Data relating to 104 travel customers was inadvertently mailed to a marketing agency without appropriate encryption. The data was not transferred elsewhere and confirmation of the deletion of this email was confirmed. The staff member is currently subject to a POL HR process. POI Management note the group-wide need to have a more appropriate culture around data security. To this end it is increasing internal staff awareness and training and is also working with the Group CISO on further tightening controls which govern external data transmission.
5. **Risk Management** - SMCR implementation is now complete. The project came in on time and under budget. POI continues to run off the TIF relationship in accordance with the agreed run-off arrangement. Less than c.5,000 TIF policies are now remaining.
6. **Vulnerable Customers** - Work to create a clearer and more descriptive vulnerable customer flag within our key trading systems is being scheduled as part of our change plan. Timescales for this work should be agreed by the end of January.
7. **GI Pricing** - The POL ARC received a comprehensive update on emerging FCA thinking in our update to the last Committee. POI will continue to review our approach as further FCA policy emerges, as well as ensuring our current approach results in fair outcomes for customers in line with our pricing policy. No further FCA output has been produced at this stage and POI continues to maintain a watching brief.

POST OFFICE LIMITED AUDIT AND RISK COMMITTEE MEETING
Strictly Confidential



MINUTES OF A MEETING OF THE AUDIT AND RISK COMMITTEE OF POST OFFICE LIMITED HELD ON MONDAY 25 NOVEMBER 2019 AT 20 FINSBURY STREET, LONDON EC2Y 9AQ AT 16.00 PM

3.1

Present:	Carla Stent	Chair (CS)
	Tom Cooper	Non-Executive Director (TC)
	Ken McCall	Senior Independent Director (KM)
In Attendance:	Nick Read	Chief Executive Officer (NR)
	Alisdair Cameron	Chief Finance and Operations Officer (AC)
	Ben Foat	General Counsel (BF)
	Andrew Paynter	Group Audit Partner, PwC (AP)
	Sarah Allen	Group Audit Senior Manager, PwC (SA)
	Rosie Clifton	Group Audit Manager, PwC (RC)
	Johann Appel	Head of Internal Audit (JA)
	Jenny Ellwood	Risk Director (JE)
	Paul Beaumont	Head of Financial Services Regulation and Compliance (PB)
	Tom Lee	Head of Finance, Financial Accounting and Controls (TL)
	David Parry	Senior Assistant Company Secretary (DP)
	Edward Dutton	Interim Managing Director PO Insurance (ED) (item 2)
	Shikha Hornsey	Group Chief Information Officer (SH) (item 4)
	Tony Jowett	Chief Information Security Officer (TJ) (item 4)
	Amanda Jones	Retail Director (AJ) (item 7)
	Cathy Mayor	Finance Director, Retail (CM) (item 7)
	Sally Smith	Money Laundering Reporting Officer & Head of Financial Crime (SS) (item 8) via telephone
	Chris Russell	Head of Data Protection and Information Rights & Data (CR) (item 11)
	Nigel Boardman (Observer)	Audit and Risk Assurance Committee Chair, BEIS (NB)
	Mark Baldock (Observer)	Head of Change Risk and Assurance (MB)
	Hugo Sharpe (Observer)	IA Audit Partner, Deloitte (HS)
Apologies:	Tim Franklin	

Action

1. Welcome and Conflicts of Interest

- 1.1 The Directors declared that they had no new conflicts of interest in the matters to be considered at the meeting in accordance with the requirements of section 177 of the Companies Act 2006 and the Company's Articles of Association.
- 1.2 The Chair welcomed observers NB, MB and HS and advised that all papers were taken as read.

2. Update from Subsidiaries

ED provided a quick overview of the key issues discussed at the recent Post Office Insurance (POI) Audit and Risk Committee meeting of 19 November:

- Whilst overall sales quality had improved, simple issues remain such as not discussing the wider POI protection product range. Management focus would be on enhancing training and working on a clearer channel strategy for the branch network.
- Over 50s insurance remains a key area of sales, however term assurance sales would be reviewed due to compliance issues, and the Easylife insurance product would be withdrawn for sale from 1 January 2020 due to poor sales.

POST OFFICE LIMITED AUDIT AND RISK COMMITTEE MEETING
Strictly Confidential



3.1

- The Senior Manager and Certification Regime (SMCR) programme (effective 9 December 2019) is on track and a revised structure plan has been accepted by the FCA.
- In line with best practice and following updated FCA guidance, it was agreed that POI would formally record customer vulnerabilities via a systems flag at the point of sale.
- Being a current issue of industry debate, general insurance pricing was discussed more formally at Board rather than ARC. POI's key influence on price was the commission added to net premiums, which on average are well within accepted limits. However, regulatory focus on limiting the commission that could be charged to the policy meant a watching brief would remain. More sophisticated pricing limits are to be considered.
- The Board also noted that the regulator was considering a number of broad market based actions (such as automatic renewals) to limit detriment to long standing customers. This would be kept under review.

3. Minutes and Matters Arising

3.1 The minutes of the meeting of the Audit and Risk Committee held on 23rd September were **APPROVED** and **AUTHORISED** for signature by the Chairman.

3.2 Progress with the completion of actions as shown on the action log was **NOTED**.

3.3 The draft minutes of the Risk and Compliance Committee held on 7 November 2019 were **NOTED**.

4. Cyber Security Update

4.1 TJ reported that following completion of Deloitte's recommendations, focus had been on reducing the maturity gap between the current and target maturity - reduced by 54% since the last Committee meeting. The project remained on track to be completed in March 2020 with an internal audit review of the work completed to date in April 2020.

4.2 The team had commenced a project to refresh the Cyber Strategy along with a data loss prevention pilot. Initial findings from the pilot had identified a member of staff in POI, sharing customer records non-maliciously as part of a group MBA project. It was noted that personal details of the customers had been deleted.

4.3 TJ advised the member of staff involved had initially been suspended with the regulators (ICO, FCA) informed of the breach, and subsequently given a final written warning. Group members (those on the MBA project) had also confirmed they had deleted the data.

4.4 In view of the records impacted (c.19,000 customer records), KM believed the suspension was too lenient and that a stronger message should be communicated to the business. Both AC and NR noted the decision was made by POI management, but recognised that future tolerance levels could be reviewed.

4.5 The Committee also discussed joiners, movers and leavers. Whilst progress has been made to introduce more rigorous procedures for employees, concern remains that consultants who no longer worked for POL still have access to the POL emails and systems. A review would be completed.

5. Contract Management

5.1 BF explained that contracts management within POL was poor and required improvement. A decentralised model would be introduced placing accountability on relationship managers for the contracts journey/lifespan.

POST OFFICE LIMITED AUDIT AND RISK COMMITTEE MEETING
Strictly Confidential



3.1

- 5.2 The Committee agreed the approach was sensible, but raised a number of concerns:
- Funding, both financial and cultural was required before the framework could be implemented.
 - Accountability - who would be accountable for the Top 50 contracts i.e. those that had the greatest financial and strategic value. Surely it should be a GE member?
 - A number of key contracts were missing from the Top 50 list, including the shareholder agreement between BEIS and POL; POL's funding agreement with the Government and the FRES contract.

- 5.3 The Committee requested the following:

1. That the top 50 list be reviewed and an update paper presented in March 2020.
2. That the full accountability matrix based on the RACI principles should be compiled and presented to the Committee. It was discussed and agreed that this should be extended to all functions (not just contract management). The Operational Risk team will assist NR.
3. That the Auditors (both external and internal) provide any examples of best practice that could be implemented.

Action:
BF

MB / NR

**PwC/
Deloitte
Action:
AC**

- 5.4 It was **AGREED** that AC would obtain funding for the contract management framework.

6. Designation as an Accountable Person (AP)

- 6.1 The Committee noted NR was POL's AP responsible for the governance, decision making and financial management of POL under the terms of Her Majesty's Treasury's Managing Public Money. He would be called to give evidence to Parliament if summoned.

- 6.2 An annual update alongside the ARA would be produced to provide assurance to the Committee and Shareholder that the AP's responsibilities had been met.

7. Commercial Partner Contingency Paper (McColls)

- 7.1 AJ explained this was a follow up to September's Committee discussion, where McColls had been identified as a partner of concern i.e. at increased risk of financial instability. McColls is a partner of considerable importance, with a current POL estate of 615 (+27 outreach) branches serving 600,000 customers a week, generating £32m of POL income per annum.

- 7.2 CM advised that a business decision had been made not to subscribe to Thomson Reuters information service, as the insight information provided would not impact/affect POL's mitigating actions should a partner cease to exist.

- 7.3 With support from insolvency specialists (KPMG), the team had developed a number of scenario based events and POL's mitigating actions where a commercial partner became insolvent or went out of business. AJ advised that focus would be on re-opening branches as soon as practically possible, however, where sites could not be re-opened, the site would be secured and cash removed from the premises. Workshops are planned to test response plans.

- 7.4 The Committee questioned:

1. Whether a subscription service should be taken with a credit agency/insurer to provide insight information;
2. How POL could de-risk itself over the next three years. In view of the size of McColl's estate, KM questioned whether a strategic review to cap partner estates (to reduce the risk and impact on POL) should be completed by the POL Board.

POST OFFICE LIMITED AUDIT AND RISK COMMITTEE MEETING
Strictly Confidential



3.1

7.5 In view of the Christmas trading period, the Committee **AGREED** an update paper should be presented in March (2020) to include results from planned test response workshop. **Action:**
AJ

8. Consolidated Report from Risk, Compliance and Internal Audit departments

Risk

8.1 JE presented an update on POL's current risk profile with the following key risks discussed:

- PCI Compliance;
- People;
- Payzone;
- Brexit and the general election.

8.2 *PCI Compliance*

The project remains red due to the lack of progress, outstanding detailed plans and no realistic alternate solutions available. Changes in senior management at Ingenico had also delayed priority talks with the CEO. It was noted that members of the Committee had discussed this subject in detail at a dedicated meeting.

8.3 *People*

JE advised that there is concern the corporate memory could be lost following the introduction of the spans and layers work. It was noted that the RACI framework (referred to in 5.3(2) above would assist in ensuring that responsibilities were understood and that handover was effective.

8.4 *Payzone*

Good progress had been made in the development of Payzone's risk management framework, risk appetite statements and risk register. A dedicated POL business partner for Payzone had been introduced.

8.5 *Brexit and the general election.*

Planning and regular meetings with BEIS for a 'no deal' exit continue. Depending upon general election results, the Committee noted that POL may be required to change its mails process between the UK and Northern Ireland, and that the new Government's position on POL may change.

8.6 Archer: JE advised that an advisory review by Deloitte of the phase 1 of the Archer development work was satisfactory.

Compliance

8.7 SS highlighted the following key compliance issues.

8.8 *Text Relay*

The team has responded to Ofcom's requests for information and that the regulator remained open to reaching a settlement rather than issuing a penalty.

8.9 *Fit & Proper*

As at 13 November 2019, 100 branches remained non-compliant (cf 186 in October) with 85 branches being de-registered from HMRC. The Committee noted and thanked the team for the progress made.

8.10 *External Threats – banking framework*

As a result of a spate of complex criminal banking deposit cases valued at £16m (where cash deposited at POL branches is subsequently used for criminal activity), the Financial Crime

POST OFFICE LIMITED AUDIT AND RISK COMMITTEE MEETING
Strictly Confidential



3.1

team visited 52 sites in London in October to raise awareness of the importance of completing suspicious activity reports. (London was selected due to the majority of incidents occurring in London.)

- 8.11 Branch feedback had been positive, but greater awareness and monitoring is required within POL and POL's partner banks.

- 8.12 *Gambling Commission – vulnerable clients*
SS noted the regulators stronger approach to organisations that had failed vulnerable clients. In view of the change, a business decision had been made to withdraw a number of National Lottery scratch-cards for sale. (Currently there are no limits on the number of scratch-cards that can be sold to customers and no guidance issued to staff when dealing with vulnerable customers.)

Internal Audit

- 8.13 JA reported good progress had been made with the delivery of the 2019/20 IA programme, with 11 audits finalised since the last Committee meeting. **Approval was sought, and given,** to postpone the Branch Cash Forecasting IA to the 2020/21 IA programme to allow for the current re-engineering of the process and to embed new controls.

- 8.14 The following IA's were discussed.
Data Analytics

The Committee noted AC's comments that the report findings did not present a positive image. Progress had been made with the appointment of a new head of data. (The work relationships between the previous teams now disbanded had broken down; GE recognised that MI, data governance required improvement.)

- 8.15 The Committee requested learnings be taken away.

- 8.16 *Employee expenses*
JA advised that a follow-up audit on Employee Expenses had found an improved control environment (previously recorded as red in 2018/19). Remedial work had been completed and a new Travel and Expenses policy published and communicated to staff.

- 8.17 *Payzone Control Environment*
JA reported the control environment within Finance and IT functions at Payzone was as a whole mostly sound and fit for purpose. A separation project from the previous owners remains on track.

- 8.18 There are no IA actions overdue ;and the Committee commended the teams on achieving this.

9. Policies for Approval

- 9.1 The following policies were **APPROVED**:
- Change Management Policy – subject to the inclusion of POMs into the group policy.
 - Personal Data Protection Policy.
 - Risk Policy.

- 9.2 The Committee requested the Risk Appetite Statement be circulated to the Committee.

Action:
JE

10. Pension Scheme Controls

POST OFFICE LIMITED AUDIT AND RISK COMMITTEE MEETING
Strictly Confidential



3.1

- 10.1 It was noted that there had been no breaches to draw to the Committee's attention.
- 11. UK Data Protection Act (including GDPR) Compliance Status Report**
- 11.1 CR explained that whilst POL was not 100% compliant with GDPR, he was comfortable with the current position noting POL was on par with/ahead of most organisations. There are two areas for remediation being contract remediation (with 12 contracts considered high risk) and the measurement and demonstration of on-going compliance.
- 11.2 Regarding compliance with the Data Protection Act 2018, the work had been split into two phases, the first concentrating on the use of customer data (now completed) and the second on updating administrative processes and controls.
- 11.3 Work on Phase 1 had been reviewed by PwC with no significant failings found and phase 2 was in transit and included contract remediation (as mentioned above).
- 11.4 He further advised that all incidents and breaches reported to the ICO had been found to be in POL's favour.
- 12. Post Office Limited Audit Strategy Memorandum (Year ending 29 March 2020)**
- 12.1 AP presented an update on the POL audit for year ending 29 March 2020.
- 12.2 He remarked the audit risk was similar to last year but had two significant risks of Group Litigation and Going Concern (to reflect the expiry of current shareholder funding in March 2021), and a number of elevated risks:
- Risk of management override of control;
 - Fraud in revenue recognition;
 - Impairment of intangible assets subject to amortisation;
 - Impairment of fixed assets.
- 12.3 Overall materiality had been provisionally set at **IRRELEVANT** slightly higher than 2018/19 at **IRRELEVANT** and that the Committee would be advised of any uncorrected misstatements in excess of **IRRELEVANT** (2018/19: **IRRELEVANT**).
- 12.4 The audit would be completed via a balanced robust approach: testing systems, transactions and the control environment and also reviewing systems identified as critical for the revenue business cycle (Horizon Online system and CFS).
- 12.5 POI and Payzone Bill Payments Limited are not significant components for the purposes of the Group audit (but are separate legal entities subject to audit by PwC in parallel / thereafter). However the POI goodwill balance within POL is material and will be subject to review as part of the POL Group audit. Gary Shaw (POI engagement leader) will provide support in this regard. KPMG are the statutory auditors of the FRES joint venture and in view of its materiality to POL's results, PwC will instruct KPMG to perform a full scope audit of FRES as part of the POL Group audit.
- 12.6 He noted the fee proposal is under discussion and did not believe the Group Litigation should affect the signing of the ARA.
- 13. ARC Meeting Dates 2020 – 2021**
- 13.1 The Committee noted the meeting dates.
- 13.2 An additional meeting would be arranged in June 2020 to deal solely with the ARA.
- 14. AOB**

POST OFFICE LIMITED AUDIT AND RISK COMMITTEE MEETING
Strictly Confidential



- 14.1 The Chair thanked JE for her contribution to ARC and POL and wished her well in her future endeavours.
- 14.2 NB thanked the Chair and the Committee for the opportunity to observe the meeting, noting that the complexity and breadth of topics that were discussed in an open, informative and transparent manner.
- 14.2 There being no further business, the meeting was closed.

3.1

.....
Chairman

Date

Actions from meeting

Minute	Action	Lead	Due Date
5.3	Contract Management The Committee requested the following: <ol style="list-style-type: none"> 1. That the top 50 list be reviewed and an update paper presented in March 2020. 2. That the full accountability matrix based on the RACI principles should be compiled and presented to the Committee. It was discussed and agreed that this should be extended to all functions (not just contract management). The Operational Risk team will assist NR. 3. That the Auditors (both external and internal) provide any examples of best practice that could be implemented. 	Action: BF MB/ NR PwC/ Deloitte	March 2020
5.4	Contract Management It was AGREED that AC would obtain funding for the contract management framework.	Action: AC	
7.5	Commercial Partner Contingency Paper (McColls) In view of the Christmas trading period, the Committee AGREED an update paper should be presented in March (2020) to include results from planned test response workshop.	Action: AJ	March 2020
9.2	Policies for Approval The Committee requested the Risk Appetite Statement be circulated to the Committee.	Action: JE	ASAP

POST OFFICE LIMITED AUDIT AND RISK COMMITTEE MEETING
Strictly Confidential



MINUTES OF A CLOSED MEETING OF THE AUDIT AND RISK COMMITTEE OF POST OFFICE LIMITED HELD ON MONDAY 25 NOVEMBER 2019 AT 20 FINSBURY STREET, LONDON EC2Y 9AQ AT 15.30 PM

3.2

Present:	Carla Stent	Chair (CS)
	Tom Cooper	Non-Executive Director (TC)
	Ken McCall	Senior Independent Director (KM)
In Attendance:	Nick Read	Chief Executive Officer (NR)
	Alisdair Cameron	Chief Finance and Operations Officer (AC)
	Andrew Paynter	Group Audit Partner, PwC (AP)
	Shikha Hornsey	Group Chief Information Officer (SH)
	David Parry	Senior Assistant Company Secretary (DP)
Apologies:	Tim Franklin	

Action

1. PCI-DSS

1.1 The Chair advised the purpose of the meeting was to discuss the Committee's ongoing frustration with PCI compliance and sought to understand what plans/solutions were in place to meet compliance.

1.2 Following a meeting with Ingenico in October, SH had been provided with assurance that POL was considered to be a high value client, and would be afforded their "Hypercare" package.

1.3 SH believed Ingenico fully understood POL's requirements and that the correct solution was now being developed but remained concerned that the poor levels of communication between POL and Ingenico continued to hinder progress. The new solution/proposal was subject to increased costs and timelines for compliance, compliance was now projected for Q1 2021 (original plan was for completion in Q1 2020) and costs for implementation had increased by IRRELEVANT

1.4 Noting the above concerns, the Committee sought to understand the following:

Action:
NR

1. Had CEO level talks taken place, as previously requested by the Committee?
No CEO level talks had not taken place due to senior management changes at Ingenico, however NR recognised these must now be completed. **Action: NR to arrange CEO level meeting as soon as possible.**

2. Are there any credible alternative providers who could provide the bespoke model POL required?
There were no credible alternative providers for the combined activity that POL undertakes although there are realistic standalone models that would be suitable for POL but would not provide an integrated solution.

3. Should Ingenico be unable or unwilling to meet compliance, was a Plan B in place and should internal resource be provided to enhance compliance?
Yes a plan B was in place, but SH had concerns with timeframes for completion. The use of internal resource was an option under consideration and needs to be discussed in more detail with Ingenico. **Action: NR to discuss in the CEO to CEO meeting.**

NR

1.5 The Committee noted the project was in a critical phase. As there was no known credible alternative integrated solution, a parliamentary question had been received on the status of POL's PCI compliance and the costs and timeframes for compliance had increased, POL would be taking a significant risk accepting the new proposal.

POST OFFICE LIMITED AUDIT AND RISK COMMITTEE MEETING
Strictly Confidential



3.2

The Committee expressed real disappointment with the programme and the level of engagement by Ingenico. After discussion, it was agreed that the CEO to CEO meeting was critical to establishing the level of engagement and confidence around a final implementation date, hopefully earlier than Q1 2021. Thereafter, careful communication of the status would be required, internally and externally.

- 1.6 KM suggested that a one off contract (under English law) be drafted for the new proposal with significant penalties for non-compliance. He queried whether the gesture of a goodwill bonus would ensure compliance.

- 1.7 TM sought to understand whether IP rights could be purchased and by when.

2. Next Steps

- 2.1 Noting discretion was essential, the following was **AGREED**:
- | | |
|--|----------------|
| 1. NR to arrange CEO level talks with Ingenico as soon as possible. | Action: |
| 2. Plan B to be investigated further. | NR |
| 3. Consideration should be given to a goodwill bonus along with a separate contract drafted under English law for the new proposal only. | SH |
| 4. NR to discuss timeframes, and use of internal resource in CEO to CEO talks. | SH |
| 5. Consideration to be given to the acquisition of IP rights. | NR |
| | SH |
- 2.2 There being no further business, the meeting was closed.

.....
Chairman

Date

Actions from meeting

Minute	Action	Lead	Due Date
2.1	Noting discretion was essential, the following was AGREED : 1. NR to hold CEO level talks with Ingenico. 2. Plan B to be investigated further. 3. Consideration should be given to a goodwill bonus along with a separate contract drafted under English law for the new proposal only. 4. NR to discuss timeframes, and use of internal resource in CEO to CEO talks. 5. Consideration to be given to the acquisition of IP rights.	NR SH SH NR	ASAP

Post Office Limited – Audit, Risk and Compliance Committee Actions List
Updated 21.01.20

REF.	ACTION	ACTION OWNER	DUE DATE	STATUS	OPEN / CLOSED
25 November 2019					
5. Contract Management					
5.3	BF to review and present Top 50 contracts i.e. those with the greatest financial and strategic value.	BF	March 2020	Under review and on-train.	Open
5.3	MB/NR That the full accountability matrix based on the RACI principles should be compiled and presented to the Committee. It was discussed and agreed that this should be extended to all functions (not just contract management). The Operational Risk team will assist NR.	MB/NR	March 2020	An updated matrix will be presented once NR confirms his new management structure and accountabilities.	Open
5.3	Auditors to provide examples of best practice for contracts management.		March 2020		Open
7. Commercial Partner Contingency Paper (McColls)					
7.5	An update paper on how POL would de-risk itself over the next 3 years. Whether a strategic review to cap partner estates (to reduce the risk and impact on POL) should be completed by the POL Board.	AJ	March 2020		Open
23 September 2019					
5. PCI-DSS					
5.6	NR to hold talks with CEO of Ingenico to progress PCI compliance.	NR	November	There has been a change in leadership at Ingenico. Shikha Hornsey to provide further details in PCI-Compliance update. NR spoken to Ingenico on 17 December 2019.	Recommend for closure.
5.6	TC to hold talks with his French counterparts to progress PCI compliance	TC	November		Open
5.6	An update on PCI compliance including commercial figures would be presented at the October Board meeting.	SH	October	There has been a change in leadership at Ingenico. Shikha Hornsey to provide further details in PCI-Compliance update.	Recommend for closure.
6. Transformation Office Changes					

Post Office Limited – Audit, Risk and Compliance Committee Actions List
Updated 21.01.20

6.5	Consider the prioritisation of the change portfolio at the POL Board	DZ	January 2020	To be included in January Board agenda.	Open
29 January 2019					
6. Money Laundering Reporting Officer (MLRO) Annual Report					
6. (a)	To provide regular updates on the complete fit and proper data to HMRC.	Nick Boden/ Sally Smith	Ongoing	Ongoing until project close. Item included on ARC agenda.	Open
7. Security Strategy					
7. (a)	To provide quarterly reports to the ARC showing how we were performing against the metrics agreed to implement the Security Strategy once the deep dive with Deloitte had taken place.	Rob Houghton / Mick Mitchell	May 2019	Ongoing. Item included on ARC forward agenda.	Open
9. Audit Strategy Memorandum	To consider a deep dive on Successfactors given the cost of the system and its limited functionality.	Exec	May 2019 July 2019	Proposals for deep dives and the sequencing of these will be brought to the May ARC meeting. Proposals will now be brought to the July ARC meeting.	Open



3.4

POST OFFICE LIMITED RISK AND COMPLIANCE COMMITTEE

Minutes of a Risk and Compliance ("RCC") meeting held at
Finsbury Dials, 20 Finsbury Street, London EC2Y 9AQ
on 14 January 2020 at 14.00 pm

Present:	Alisdair Cameron (Chair) (AC)	Chief Financial Officer
	Nick Read	Chief Executive Officer
	Ben Foat (BF)	General Counsel
	Shikha Hornsey (SH)	Group Chief Information Officer
	Cathy Mayor (CM)	Finance Director, Retail (deputising for Debbie Smith)
	Stephen O'Reilly	HR Director - Business Partnering & Recruitment (deputising for Lisa Cherry)
	Chrysanthi Pispinis (CP)	Post Office Money Director (deputising for Owen Woodley)
In Attendance:	Johann Appel (JA)	Head of Internal Audit
	Mark Baldock (MB)	Head of Risk
	Jonathan Hill (JH)	Compliance Director
	Tom Lee (TL)	Head of Finance, Financial Accounting and Controls
	David Parry (DP)	Senior Assistant Company Secretary
	Tony Jowett (TJ)	Chief Information Security Officer (items 4, 5)
	Meredith Sharples (MS)	Director, Telecoms (items 6.15 -)
	Barbara Brannon (BB)	Procurement Director (item 7)
	Mark Dixon (MD)	Head of Treasury, Tax & Insurance (item 8)
	Dan Zinner (DZ)	Chief Transformation Officer (item 9)
	Sally Smith (SS)	Money Laundering Reporting Officer and Head of Financial Crime (item 10)
	Tim Armit (TA)	Business Continuity Manager (item 11)
Apologies	Lisa Cherry, Group HR Director; Shikha Hornsey, Group Chief Information Officer; Debbie Smith, Chief Executive Retail; Owen Woodley, CE Financial Services & Telecoms;	

1. Welcome and Conflicts of Interest**Actions**

- 1.1 AC opened the meeting and advised that papers would be taken as read.
- 1.2 The Directors declared that they had no new conflicts of interest in the matters to be considered at the meeting in accordance with the requirements of section 177 of the Companies Act 2006 and the Company's Articles of Association.

2. Minutes and Action Lists

- 2.1 The minutes of the RCC meeting held 7 November were **APPROVED**.
- 2.2 Progress on completion of actions as shown on the action log was **NOTED**.

3. PCI-DSS Update

- 3.1 Due to illness, an update on PCI-DSS would be provided by SH to GE (General Executive) on Monday 20 January 2020.

4. Cyber Security

- 4.1 TJ provided an update on Cyber Security. He reported that currently POL performs routine testing for table top incident response exercises, red team testing, penetration testing and vulnerability scanning. JA confirmed that the internal audit found that good progress had been made in enhancing POL's cyber maturity with no real areas of concern for noting.
- 4.2 NR received confirmation that POL (and its subsidiaries) could be held to a ransomware attack as had recently happened with Travellex. TJ advised that in this scenario, payment would not be made, and that POL would look to bypass the attack and start again. Data was backed-up on a daily basis.



3.4

- 4.3 BF queried whether POL should be benchmarked against other government owned organisations and what POL's level of maturity compared was to these organisations. NR advised that as part of the Deloitte review of cyber security, a decision had been made for POL to benchmark against Financial Services and Retail organisations/institutions rather than government owned institutions. There were no plans to benchmark against government institutions.
- 5. Policies for Approval – Cyber and Information Security Policy**
- 5.1 The Policy was approved.
- 5.2 It was noted the policy was an amalgamation of the IT Security, Acceptable Use and the Document Retention and Disposal policies. This was to avoid duplication, to provide one source of information, and to align the policy with current cyber security needs.
- 6. Combined Risk, Compliance and Audit Update**
- Risk**
- 6.1 The top risks of PCI, Retail Proposition, Group Litigation, IT Technology and Interruption, People, Business Continuity, Payzone and Brexit were noted, with the following points discussed.
- 6.2 **PCI Compliance** – the project remained “Red” overall against current plan. Compliance was now expected in Q1 2021 and plans and costs from Ingenico remained outstanding.
- 6.3 **Retail Proposition** – MB advised that some agents considered POL costly, complex and unattractive to join, however it was noted recent increases in agent remuneration should improve branch sustainability.
- 6.4 **Group Litigation** – BF advised that the class action had closed, but that the litigation remained ongoing. The risk remained post settlement.
- 6.5 **Brexit** – fortnightly meetings with BEIS continued. MB noted the process to process mails between the UK and Northern Ireland post Brexit may need amending to allow for the completion of EU custom declaration forms for post being sent from UK to Northern Ireland.
- Compliance**
- 6.6 **PSD2 Implementation** – PSD2 (Payment Services Directive 2) is an EU directive aimed at improving consumer rights and enhancing online security which came into force in January 2018. Initial legal advice received had advised that the directive did not apply to POL, however, subsequent legal advice countered this claim.
- 6.7 The Committee queried the lack of urgency in making the necessary changes required, and questioned why the regulator had not been informed of non-compliance. NR and AC requested that as a matter of urgency, the regulator be informed (to avoid a repeat of the Text Relay Issue). BF advised a letter for Meredith Sharples to be sent to the regulator yesterday had been approved by Legal.
- 6.8 A separate paper on PSD2 would be discussed later in the meeting.
- 6.9 **Data Protection** (review of cookie approach) – recent guidance from the Information Commissioners Office clarified the management of cookies on the Internet and Applications which had identified that POL was non-compliant. The Digital, Legal and Data Protection teams are working on solutions to mitigate this issue and a paper is to be presented to the GE in January. BF requested that industry literature and third party assurance be sought.
- 6.10 **Contract Remediation** – further analysis had identified 199 additional contracts that required remediation. The programme is planned to conclude in July 2020. The Committee questioned who was accountable.
- 6.11 **Video and Mystery Shopping** – issues with video and mystery shopping remained for example the non-disclosure of medical information and product information. In view of the lack of progress, AC proposed a management decision is required on whether services should be withheld/withdrawn from branches until compliance improves.
- 6.12 AC remarked that consideration was required on whether management time should be spent on improving the first line of compliance and contracts management, and whether the second line sits within the business. He noted either stronger business ownership is required or a stronger central function is required.
- Internal Audit**
- 6.13 The following points were raised:
- 6.14 Good progress had been made with the audit plan for 2019/20 with three audit reviews finalised since the last ARC meeting (25 November 2019), these being PCI Programme, Cyber Security and CFS Controls (Post Back Office Transformation (BOT)). As at 6 January 2020, 47 actions remained open with three overdue – FS Training, Purchase to Pay and Payzone Controls.
- 6.15 CM raised concern with the lack of bandwidth in Payzone and the poor second line of command.



3.4

- 6.16 **Payment Services Directive 2 (PSD2) Implementation** - Regulated by the FCA, MS reported PSD2 came into effect in January 2018 for companies that bill customers who use premium rate call services. POL had received conflicting legal advice (initially stating the regulation did not apply to POL, subsequently challenged and found to apply) and advised that recent correspondence from the regulator to remind companies of their obligations.
- 6.17 At present POL could not cap some of these bills, and whilst there was a distinct possibility of a penalty for non-compliance, urgent work was underway with Fujitsu to find a solution.
- 6.18 The Committee sought assurance that there would be no repeat of the Text Relay issue (recognising this would be a separate issue) and that the lack of urgency was a concern. The letter prepared by BF (advising of non-compliance) should be sent to the regulator today. **Action: MS**
- 7. Supplier Contracts out of Governance**
- 7.1 BB reported there had been 11 new non-compliant incidents since the last RCC meeting (7 November 2019) valued at [IRRELEVANT] and noted that currently, there are 28 non-compliant incidents totalling [IRRELEVANT], with over half (56%) in Retail. The following contracts in the pipeline were considered high-risk:
- 7.2 **SSK funding** – this is an [IRRELEVANT] annual support contract that continues to non-compliantly roll over until replacement and updated SSK machines are purchased.
- 7.3 **Brands/RAPP** – this is an [IRRELEVANT] contract extended to April 2020. A business strategy, funding and sourcing plan needs agreement.
- 7.4 **Media Planning** – this is an [IRRELEVANT] contract due to expire in April 2020. It was noted the preferred Marketing option to complete an OJEU process is not achievable in the timeframe and a period of non-compliance (6-7 months) would be required. AC questioned which forum would be best to make a decision.
- 7.5 **Global Payments** – this is an [IRRELEVANT] contract due to expire in May 2020. An extension would be required for 12-24 months until a new provider could be found. A discussion on this was to be held at GE (January 2020).
- 7.6 The Chair reminded the Committee of POL's obligation to adhere to the Public Contract Regulations 2015 and requested the requirement for tighter controls on contracts management be re-iterated in team meetings.
- 8. Tax Update and Annual Tax Strategy**
- 8.1 MD presented the latest tax update for the financial year 2018/19. Focus has been on embedding back office transformation changes, integrating Payzone into the VAT group, and VAT reporting. Significant progress has been made on improving controls around VAT and removing a number of manual controls with automated controls.
- 8.2 Regarding employees considered to have more than one permanent place of work (mostly senior employees, paragraphs 12 and 26 of the report), an underpayment of benefit-in-kind tax had been identified, and it was possible the regulator could levy a penalty of up to 15% tax underpaid. This would be kept under review and the contractual position of employees affected would appropriately be changed. AC recommended that MB liaise with SR and TL.
- 8.3 Regarding IR35 changes to the employment status of contractors, Deloitte was assisting with a review of contractor status where it had been found that some contractors should have been listed as employees. The regulator had been informed.
- 8.4 The Annual Tax Strategy was noted.
- 9. Transformation Office Changes**
- 9.1 DZ reported that since the last update in September, financial controls had been established for CapEx and Exception spend, with set limits tracked by Strategic Portfolio Office (SPO) which avoided spend over approved limits occurring and the development of stronger governance controls.
- 9.2 A transformation team was now embedded into the role and weekly and monthly updates are provided to GE and UKGI respectively.
- 9.3 He explained that work is required on "people understanding" in terms of communication, training, induction and the conviction for change processes and governance, and that the SPO was currently working with IA to define, develop and refine the current Change controls framework.
- 10. Money Laundering Reporting Officer (MLRO) Annual Report**
- 10.1 SS explained that the annual report was a legal requirement to appraise senior staff of the effectiveness of POL's key anti-Money Laundering and counter terrorist financing controls in place, and to make any suggestions for improvement if required.
- 10.2 She advised there had been greater regulatory focus and scrutiny on money laundering and terrorist financing, with a more proactive approach to supervision and the issuing of penalties by HMRC. It was



3.4

- noted a new HMRC supervisor was expected in the early part of 2020 which may change the current business relationship, and that the team had been expanded to meet increased workloads.
- 10.3 Key areas of work for the department included Fit and Proper returns (which remained a challenge), Bureau de Change residual risk, assurance activity for Payzone products and services and the review of high value and high profile investigations relating to money laundering through Post Office counters. There had been a significant improvement in mandatory training compliance in the Network.
- 10.4 She advised that whilst the framework for anti-money laundering and counter terrorism funding controls was generally effective, greater focus was required on the completion and maintenance of Fit and Proper returns, reviewing suspicious activity relating to banking deposits, and greater consideration towards increased regulatory scrutiny and penalties. Attention was also required on ensuring key compliance messages were understood and acted upon, and that the first line was aware of its responsibilities.
- 10.5 AC requested the paper provide examples of the actions POL had and would be undertaking to meet its regulatory obligations over the next 12 months and that management consideration was required by management on investing in a stronger compliance function or changing culture to ensure people understood their obligations/responsibilities. The MLRO report for Post Office Management Limited was noted.
- 10.6 AC requested BF, SS and JH talk to retail on enforcing three lines of defence and suggested BF attend a meeting with HMRC. **Action:**
BF, SS, JH
- 11. Business Continuity Update**
- 11.1 TA presented the latest Business Continuity update. Whilst he was comfortable with the current position, he noted there had been a number of unrelated serious IT issues before Christmas, possibly due to departmental changes and poor change controls in place.
- 11.2 His concerns included a significant partner failure, what would happen to Horizon should it fall over, Fujitsu, and the outcome from a full shut down and re-start test of Horizon. On-going work with product teams and IT continued to ensure that systems are resilient.
- 12. Review of draft Audit, Risk and Compliance Committee meeting agenda**
The draft ARC agenda for 28 January was **NOTED**.
- 13. Any other Business**
There was no other business.



Post Office Limited Audit, Risk & Compliance Committee Report

Title:	Cyber Security Strategy Update
Meeting Date:	28 January 2020
Author:	Tony Jowett, Chief Information Security Officer
Sponsor:	Shikha Hornsey, Group CIO

4

Input Sought

Action Required: Noting	1. To note the status and plans regarding our response to recent ransomware events 2. To note the status and plans regarding Cyber testing
Previous Governance Oversight:	Actions to report on 2. Above topics occurred at the previous Risk and Compliance Committee (RCC) in November 2019.

Executive Summary

Context:	<p>The recent spate of ransomware attacks and the specific attack on Travelex have posed questions regarding the risk to us of such an event and our ability to respond. This paper describes our recent activity to reduce the likelihood and impact of such an attack on Post Office.</p> <p>Cyber testing in all its guises is key to checking cyber defences and identifying areas for improvement. At the RCC in November a request was made for an update in this area.</p>
-----------------	---

Confidential

1



Questions asked & addressed

1. How are we reducing the likelihood and impact of a ransomware attack?
2. What is the current status and plans regarding Cyber Security testing?

Report - Ransomware

4

3. Ransomware attacks aim to extort money from an organisation by encrypting data via malware and then demanding a ransom to decrypt it. Ransomware attacks are often used by terrorist and criminal organisations to raise funds for their other operations.
4. Infection usually occurs through phishing attacks or through rogue websites containing malware which impersonate real ones.
5. Once the malware has infected a computer it can stay dormant until activated remotely by the criminals. An organisation can therefore be infected months before the attack becomes obvious if the initial entry is undetected.
6. Once activated ransomware rapidly encrypts the host computer and then reaches out to all connections on the network to copy itself to other computers and start the encryption and further copying process there. Such attacks therefore spread rapidly across entire organisations if there is insufficient protection.
7. The impact of Ransomware attacks is usually severe as such encryption can prevent entire organisations from functioning depending on how widespread the attack is. As an extreme example, the 2017 Maersk Container Shipping attack stopped the entire operation from working for two months costing them an estimated \$120m in recovery costs, lost business and brand damage. There are thought to be many other smaller-scale attacks that never get reported.
8. Ransomware attacks can be difficult to recover from as, in addition to encrypting user data, ransomware can encrypt system data such as databases and active directory (which controls access to the system). Unless such data is kept in an off-line "cold" back up then there may not be a clean copy to restore to as cloud-based copies may also be encrypted.
9. Details from the recent Travelex attack are scarce as it is still ongoing, but it is thought to have occurred through infection through remote networking software. We have checked our own defences against a similar attack and strengthened appropriately.
10. Given the invasive nature of Ransomware then the recommended policy is to have defences aimed at all levels - *Protect*, *Detect* and *Recover*. Good overall cyber defences across all cyber domains are needed. We have existing robust cyber defences but given the recent increase of frequency and severity of such attacks we have increased our level of alertness and we are seeking further assurance. Therefore, we have:
 - a. Contacted our Threat Intelligence partners Recorded Futures to reassure ourselves that they are monitoring for any indicators that we are being targeted
 - b. Alerted our Verizon and in-house SOC to increase vigilance by looking for indicators of infection



- c. Asked our IT operations team to ensure anti-virus software is up to date
- d. Begun checking our off-line backup regime
- e. Contacted the FRES CIO and CISO to ask that they assure us that their defences are alert to Ransomware – we have so far received good verbal assurances regarding their defences and await the completion of follow up actions
- f. Confirmed that we have in our plans the guidance received from the National Cyber Security Centre on how to defend against Ransomware
- g. Contacted Deloitte, who have performed Ransomware recovery for several large organisations (including Maersk and Norsk Hydro) to tap into their experience of large-scale Ransomware recovery. We have asked that they scan our internet-facing estate for any malware that may already be there but laying dormant, assess our defences against current Ransomware attack types, and develop a playbook for us to respond quickly and effectively to any such attack. We expect that this work will start in late January and complete in six weeks.

11. An update on this activity will be provided at the next ARC.

Report – Cyber Testing

- 12. At the previous RCC an action was raised regarding the running of desktop incident response testing. The response to this has been widened to cover all types of Cyber testing.
- 13. Cyber testing provides the evidence that cyber defences are working well and helps identification of gaps.
- 14. The following types of testing are in use within the Post Office:
 - a. Table-top incident response exercises
 - b. Red team testing
 - c. Routine penetration testing
 - d. Vulnerability scanning
- 15. Table-top exercises aim to simulate real-life incidents and involve all key personnel in IT and Cyber operations although the scope can be widened. As the name suggests they involve the walking through of an imaginary (but realistic) incident in a meeting room with independent observation and facilitation. Such an exercise is planned for Q1 2020.
- 16. Red-team testing is invasive technical testing performed largely in secret by an external organisation. As far as possible (without doing real damage) a red team will act as if they are external attackers with a specific goal e.g., to gain access to GE email accounts. The lessons learned from red team tests are highly valuable as they simulate real-life attacks. Such a test was conducted in August 2019 and we are in the middle of conducting such a test. Findings from this will be reported back at the next meeting.
- 17. Routine penetration testing is usually performed annually for operational systems or on commissioning new systems into production as part of Change Excellence. The output from Penetration tests enable vulnerable components to be patched and fixed before live data is held by such systems.



-
18. Vulnerability scanning services routinely scan the perimeter and perimeter facing systems and report on vulnerabilities in defences. These can be automated to run continuously which, in a company that uses agile development, is essential to keeping track of new issues to resolve. These services are part of the Cyber Strategy for 2020 onwards.

4



POST OFFICE LIMITED RISK AND COMPLIANCE COMMITTEE REPORT

Title:	Payzone Bill Payments Update
Meeting Date:	28 January 2020
Author:	Michelle Embrey, Quality and Risk Manager, Payzone
Sponsor:	Andrew Goddard, Managing Director, Payzone

5

Input Sought

Action Required: Noting	To note the progress made with the Payzone risk framework and the Payzone risk register.
Previous Governance Oversight:	

Executive Summary

Context:

This paper provides an update on the progress of the risk framework and the latest risk register position. The risk workplan has been created to monitor and update the management team on progress of the key activities. This includes the progress being made to address the significant risks and return to acceptable levels.

This report highlights the 5 significant risks (a risk score of greater than 12) notably; the need to consider GDPR requirement, the integration and impact of Post Office standards within operations and commercial areas, impact of Brexit, a terminal communication issue affecting agent and customer transactions, and the risk to forecast revenues versus original acquisition forecasts. Each of these risks have a plan to resolution by end FY 2019/20.

The progress of the risk framework from the previous reporting period includes the following; Payzone management team have reviewed the risk register and agreed target risk scores with mitigation plans and target dates in place and develop a process flow chart detailing the correct risk management process has been generated and submitted to POL risk team for their review and comments.

Confidential

1



Questions asked & addressed

1. Status of the risk framework
2. What are the significant & emerging risks and what are we doing to address these?
3. What additional activities are required to embed risk into ways of working?
4. Conclusion

Report

5. Status of the Risk Framework

Work has been continuing to develop the risk management framework. The detail of which is covered below:

- a. A risk management and incident process flow chart has been created and submitted to POL risk team for review
- b. The staged approach for the full integration of a risk framework is continuing. The following stages have been completed:
 - (i) Stage one - review the residual risks from the original Panther RAID log
 - (ii) Stage two - review the risks raised during the risk workshop held in July 2019 for relevance and score
 - (iii) Stage three - review the risk register and assign target risk scores with due dates
- c. The risk appetite will be further developed with the intention to generate a risk statement by March 2020.
- d. A meeting was held on October 16, 2019 between Carla Stent and Andrew Goddard for the purpose of discussing governance and risk management within Payzone Bill Payments. As a result of this meeting and the points raised a risk work plan was created that details the key activities highlighted, summarised below:
 - (i) Risk and governance oversight as a division of POL: Complete with PZBP providing reports to the POL risk team and are a column on the placemat
 - (ii) Risk appetite of the business: Ongoing - Statement scheduled for completion March 2020
 - (iii) Material risks for Payzone: Ongoing task – The Risk register is in place and risk reviews completed on a monthly basis
 - (iv) Parent company guarantee risk note: Ongoing – Complete integration of POL and PZ bill payment teams in Q4 and agree approach to client tenders to negate the requirements for parent guarantees
- e. The purpose of this plan is to monitor and communicate the progress made on these key activities including the significant risks as detailed in the significant risk register. Mitigation and due dates have been assigned to significant risks to bring the residual risk scores to acceptable levels

6. What are the significant & emerging risks and what are we doing to address these?



a. Risk Changes

The following Tables 1 & 2 illustrate the classification of risks and issues and the progress since the September PZBP Board. In Table 1, the total number of risks have not changed and remain a total of 21, with 2 high risks actioned, 5 re-classified from previously reported as blank, and 7 new risks added in the period.

Table 1

Residual Risk Score		Low				Medium				High				Black Swan	
Risk Category	Blank	1	2	3	4	6	8	9	10	12	15	16	20	5	Grand Total
All												1		1	2
Customer & Client		1		1											2
Financial		1		1	1	1					1	1			6
IT & Operational		1	1		1				1				1		5
Legal, Regulatory & Other Requirements				1								1			2
People		1	1	1		1									4
Grand Total	0	4	2	4	2	2	0	0	1	0	1	3	1	1	21
Last Reporting Period	5	3	2	4	0	1	0	0	1	1	2	1	0	1	21
Delta	-5	1	0	0	2	1	0	0	0	-1	-1	2	1	0	0

In Table 2, the issues have remained relatively stable with a total reduction of 1 overall.

Table 2

Impact Rating	Low		Medium	High	V. High	
Risk Category	1	2	3	4	5	Grand Total
All						0
Financial						0
IT & Operational	2	1	4			7
Legal, Regulatory & Other						0
People						0
Customer & Client						0
Grand Total	2	1	4	0	0	7
Last Reporting Period	2	1	5	0	0	8
Delta	0	0	-1	0	0	-1

b. Significant Risks

The top Payzone Bill Payments risks as shown in Appendix 1 (in Reading Room) are:

i. Terminal Communication Issue - Risk score 20 (5:4)

The urgency of implementing a solution to the device communication issue, highlighted with the launch of British Gas impacts the performance of the network and customer experience in store. An operational improvement plan is in place which focuses on three actions to mitigate the risk. These consist of out bound calls to identify issues, sending engineers where needed and software fix alongside a parallel evaluation of re-designing the quantum gas card journey. The target date for returning this risk to acceptable levels is 7th February 2020.



ii. **GDPR Requirements - Risk score 16 (4:4)**

There is a need to re-assess the GDPR process requirements in conjunction with the Post Office Data Protection Team. The reappraisal of this process will be conducted by 31st January 2020 with an aim to create a process improvement document that details the areas of weakness in the GDPR process and prioritise actions with deliverable target dates. This risk has been given a high priority to mitigate and implement a process.

iii. **POL Policies and Operating Standards - Risk Score 16 (4:4)**

The adoption and integration of the PO policies and operating standards is an area of ongoing appraisal as the integration of the two businesses mature. The formulation and agreement of a risk statement will assist in determining the extent and timelines for completion of this work. A plan of integration will be created which will detail the extent to which PZBP integrate the POL policies and operating standards. The risk statement and the integration plan will be delivered by the March PZBPL board meeting, scheduled for 26th March 2020.

iv. **Forecast Revenues - Risk score 15 (5:3)**

The risk to forecast revenues from under-performing against the original acquisition business plan. The success in securing the British Gas exclusive contract and pipeline of other key clients will mitigate this risk and factored into 2020/21 business plan.

v. **Brexit - Risk Score 5 (5:1)**

Brexit has been scored as a potential black swan event. The risk to the operation is low based on an appraisal of suppliers and technology processes and the only risk relates to the broader macro economic impact to the UK economy.

7. Conclusion

- a. There is a total of 21 risks identified with 12 being low, 3 medium, 5 high and 1 black swan. Of these risks there are 6 significant risks (risk score of 12 and above).
- b. This report highlights the significant risks (a risk score of greater than 12), notably; a terminal communication issue affecting agent and customer transactions, the risk to forecast revenues from under-performing, re-assessing GDPR requirements, the integration and impact of Post Office standards within operations and commercial areas, and the impact of Brexit (see appendix 1). These risks have mitigations in place and a risk workplan has been created to monitor and update the management team on progress of the key activities. This includes the progress being made to address the significant risks and return to acceptable levels.



Appendix 1

Significant Risks

Risk ID	Risk	Impact	Controls	Residual			Assigned To	Progress Update
				Impact	Likelihood	Residual Risk Score		
RN021	Terminal communication issue. Does this become a more urgent requirement to resolve	Unable to complete quantum transactions without reboot Customer impact as they may be unable to purchase energy loss of merchants Reputational damage	Temporary work around is to reboot the equipment	4	5	20	Ralph Wort	20.01.2020 - 308 quantum efficiencies deployed and now party of the core build. 309 final release will be deployed next week. 07.01.2020 - RW There are 3 fixes currently in testing for deployment in Q1. The fixes were on hold to ensure stability of service for 1st Jan exclusive service. Quantum will be deployed on the T103 terminal Q1. 12/12/19 - A number of additional fixes are planned for deployment, however, currently on hold to ensure stability of service whilst in 5 day consecutive operation test and in readiness for 1st Jan exclusive service. Unlikely to release before mid January. Plan to be developed to communicate to retailers on resolution process
RN002	Payzone operates in a highly dynamic and low margin service market, with PO ownership having the potential to encumber Payzone operations, slowing down market response and increase costs	The business may become unprofitable in PO ownership were extensive adoption of PO standards occur without reference to cost The Finance team may become ineffective due to the unplanned and expanding requirements due to POL Governance	i) Payzone being established within PO as 'arms-length' operation with own Payzone Board and dedicated management team ii) PO corporate services will be taken where they are cost-effective and governed through a Master Services Agreement iii) Operational and financial oversight will be established from exchange	4	4	16	Damian Scholes	(PRI026) A plan of the incorporation of the POL policies and operating procedures to be completed by 26.03.2020 31.10.19 - NS: PZBP & POL currently working to improve this situation There is a requirement for POL to improve the communication and scope of work required in order to meet their requirements. The expected deliverables need to be communicated by POL in advance. 07.10.19 - DS not available for meeting, ME requested update via email 07.10.19 17.09.19 - DS Engage PO compliance team early in the contract negotiations 11.09.19 - Risk meeting update. Risk impact increased from 3 to 4 and likelihood also increased to 4 due to
RN024	There is a need to re-assess the GDPR process requirements	A breach to GDPR could result in fines proportionate and dissuasive for each individual case. GDPR has set forth fines of up to 10 million euros or up to 2% of the organisations entire global turnover of the preceding fiscal year, whichever is higher.	Controls in place include: Call recordings reports	4	4	16	Karl Taleb / Michelle Embrey	ME to review process and create improvement plan ME: Retention schedules have been created for HR, Helpdesk & Finance. Procedures are being developed with POL data protection team The data breach and information request processes are being developed in conjunction with the POL Data Protection Team 26.11.19 - KT: The focus on the MVP will be covering all the traceable functionality manually, to get it in quickly: Mapping inbound numbers and making them visible on the dialer, Blank form for Prospects on Remedy to capture and track the Prospect Journey, Implementation of the Prospect concept in Remedy, Addition of suitable disposition codes
RN001	There is significant risk to forecast revenues from under-performance of Payzone	Under-performance impacting ROCE for the transaction. Increased competitor activity, reductions in transactions volumes or increase in retailer fees could lead to a decrease in agents and subsequently a loss in clients	(i) Earn-out formula agreed whereby some of the risk associated with the revenues recognition is linked to payments to PZ. (ii) Preparing the commercial/marketing plan to be effective from Completion (iii) Implement comprehensive, pro-active, communications programme with audience specific messaging	5	3	15	Commercial	(PRI001) 01.01.2020 - British Gas now live, milestones 1 & 2 of the PGC risk note met. 07.10.19 - DS not available for meeting, ME requested update via email 07.10.19 4/9/19-MD: No change, will discuss during risk meeting. 8/8/19: Mitigating with success in negotiating exclusive contracts with BG and SP. Potential did exist but now being successful. Other clients expected to follow. 25/7/19-AG: Revenue now in line with the plan, however, costs lines greater. Statement from AG to NS which reflected this position. Chase her for this update. Technically the business isn't underperforming, costs are just greater
RN018	Brexit	Free flow of data from the EU may be restricted in the event of a no deal infrastructure in Ireland Bit wise in Holland Development team has EU nationals (1) Equipment purchased in China - Increased import tax	RW Bring infrastructure into UK Discontinue Bit Wise contract ME - receiving gov email updates on Brexit progress/changes	5	1	5B	Risk Forum	The risk to the operation is low based on an appraisal of suppliers and technology processes and the only risk relates to the broader macro economic impact to the UK economy. 07.10.19 - ME to contact Heroku regarding post Brexit plan. RW - Possible increased import tax due to current import agreements with EU not UK Black swan event

Confidential



Post Office Limited Audit, Risk & Compliance Committee Report

Title:	Tax Update and Annual Tax Strategy
Meeting Date:	28 January 2020
Authors:	Mark Dixon, Head of Treasury, Tax & Insurance Andy Jamieson, Tax Manager
Sponsor:	Alisdair Cameron, Chief Financial Officer

Input Sought

Action Required: Noting/ Decision	The ARC is asked to note the Tax Update and approve the annual review of the Tax Strategy.
Previous Governance Oversight:	

Executive Summary

Context:	As a follow up to the paper presented to the Audit, Risk and Compliance Committee in October 2018 this paper provides an update on tax, as well as on the annual review of the POL tax strategy last published in January 2019 (the "Tax Strategy").
-----------------	--

Confidential



Questions asked & addressed

1. What are the strategic tax challenges for POL?
2. What are the current key tax issues for POL?
3. What progress has been made around the changes to the tax team described in the last update?
4. What other tax updates should the ARC be aware of?
5. What is the requirement for reviewing and updating the published tax strategy?

Report

What are the strategic tax challenges for POL?

Improving control around VAT

6. As reported in the last update the primary tax risk remains around VAT and, in particular, ensuring that POL pays and claims the correct amount. This year we have focussed on: embedding the Back Office Transformation ("BOT") changes; integrating Payzone into the VAT group; and our VAT reporting. This has allowed us to further improve controls around VAT. We are compliant with HMRC's current Making Tax Digital ("MTD") requirements.
7. The BOT and MTD projects have allowed us to replace a number of manual controls with automated controls. New BI tools have been developed to implement changes to the VAT return preparation process, while also enhancing controls. HMRC's MTD Initiative (see [38] below), which includes a requirement to have "digital links" through the process, will also provide an opportunity to enhance control. Further automation is also being introduced as part of the Source to Settle procurement project. This will reduce some of the current risk associated with tax coding of purchases across the business.
8. As a result of the revised processes and controls some historical errors, which have occurred over the last four years, have been identified and reported to HMRC. Out of total tax throughput (i.e. VAT incurred and output tax payable) of over [IRRELEVANT] over the period, approximately [IRRELEVANT] was paid to HMRC relating to two main issues, however approximately [IRRELEVANT] was reclaimed from HMRC following improvements to existing processes. These corrections were reflected in the 2018/19 Annual Report and Accounts.

Protection of our VAT position

9. POL gains a VAT benefit from an agreement regarding the treatment of the income it receives from Royal Mail Group ("RMG"). It is referred to as the "Stamp Solution". The treatment was agreed with HMRC and RMG at the time of separation. It allows POL to treat the margin income received for the sale of stamps and stamp-related products as outside the scope of VAT, rather than as subject to VAT. The saving can be calculated by calculating the VAT that would be payable on the annual margin and then estimating the cost to RMG if we were to charge it. In 2018/19 the margin for VAT purposes was [IRRELEVANT] RMG's VAT recovery position was around 50% and, therefore, the VAT saving was [IRRELEVANT]
10. Changes to POL's operations should be carefully considered to ensure that the Stamp Solution is maintained. The legislation governing the treatment of vouchers (which stamps fall under) was amended from January 2019. There was no direct impact from the change.



Improving Control around Employment Taxes

Healthcare Trust

11. In 2018/19 POL paid certain additional sums into the Healthcare Trust ("HCT") to fund members' costs in areas that were out of the scope of the cover of the policy. The appropriate tax treatment was not applied to these payments. This resulted in an underpayment of benefit-in-kind tax ("BiK") and NI to HMRC covering four years. A settlement payment of [IRRELEVANT] was made in January 2019. The change in scheme provider to BUPA means that further issues of this nature should not occur.

Employees considered to have more than one permanent place of work

12. In 2019 we identified an issue whereby certain employees, who had been appointed on home-based contracts, were required to work regularly at office locations. Where there is a regular, permanent second place of work and the individual claims expenses for travel, accommodation and subsistence, it is a taxable benefit-in-kind. HMRC deem the employee to have more than one permanent place of work.
13. A payment in respect of tax was made for 18/19 as part of the normal annual settlement process and we are currently reviewing whether there has been an underpayment in tax for prior years. For 18/19 we calculated that there was an underpayment of Benefit-in-kind ("BiK") tax of [IRRELEVANT] which was reported in the annual PAYE Settlement Agreement (PSA) submission in October. We are in the process of reviewing the position back to 15/16 to correct any outstanding tax. It appears likely that similar amounts of tax may be due and is possible that HMRC may levy a penalty of up to 15% of the tax underpaid. The business will review the contractual position of affected individuals and make changes where appropriate.

6

IR35 – employment status of contractors

14. IR35 introduced legislation to assess whether a contractor should be placed on the payroll or whether they can invoice as a 3rd party. As a public sector organisation we carry out assessments, using HMRC's on line tool when engaging contractors and were required to do so from April 2017. HMRC recently introduced a revised on line assessment tool which has indicated a different outcome around certain contractors' employment status than when the original tool was used. We are currently working with Deloitte and HMRC to evaluate whether there are tax implications for us around this issue.
15. As a consequence of HMRC's on-going review of employment status of our contractor population we carried out a re-assessment of the position we have taken. Initial findings indicate that in some cases we may have incorrectly applied HMRC's tool, leading to contractors being considered not to be employees when, in fact, they should have been. Deloitte is supporting us in assessing the position and we await the outcome of HMRC's review. If we are found to have treated the employment status incorrectly we will be liable to account for underpaid tax and NI, and HMRC may look to levy a penalty. We are working towards identifying the materiality of the issue.

Deloitte review

16. Following the issues set out at paras 11 to 13 we engaged Deloitte in late 2019 to review our employment tax governance and controls. Deloitte reported that, although most processes are clear and formally documented, accountability for employment taxes was not

Confidential

3



adequately defined. They have recommended a formal governance framework is designed and implemented across employment taxes. Currently the HR Reward & Benefits team, the HRSC, the Agents Remuneration team and the Strategic Projects Office (SPO) own different parts of the processes and the central Tax team supplies support, relying on 3rd party advice for expert guidance. The Tax team will develop the governance framework with support from Deloitte and the key stakeholders of the processes.

Understanding and Optimising Corporation Tax Losses

17. As at the 2017/18 tax year POL had accumulated tax losses of [IRRELEVANT]. We estimate that, once the 2018/19 tax computation has been finalised and submitted, POL will have losses carried forward of in excess of [IRRELEVANT].
18. From April 2017 the tax loss carry forward that can be utilised is now restricted to an initial [IRRELEVANT] of profits and then 50% of the profits above [IRRELEVANT]. This means that POL will now begin to pay corporation tax sooner than it would have done under the old loss rules.
19. Despite being increasingly profitable at an EBITDAS level, POL continues to create tax losses whilst it incurs significant exceptional and transformational spend which is deductible for tax purposes. We therefore do not anticipate paying corporation tax in the very near future.
20. However, given the changes to the tax loss rules and the impact that tax may now have on project decisions it is important that we can now project future creation and utilisation of losses. We have therefore built a tax model to calculate our future position. The model allows us to understand the impact of business decisions on our tax position.

What are the current key tax issues for POL?

VAT Treatment of Post Bill Payment Processing Income

21. In the October 2018 update we made the ARC aware of certain potential changes to the VAT treatment of commissions on bill payments.
22. Our bill payments business provides POL with approx. [IRRELEVANT] of commission income per year. About 90% of this relates to "post-pay", where the customer makes a payment after receiving their bill, for which commission is VAT exempt. The rest relates to "pre-payments" for which commissions are standard rated. Our largest clients for "post-pay" are Santander and AllPay and together they represent about 50% of the income.
23. In 2017, following a VAT tribunal case involving PayPoint, HMRC queried whether we should apply the standard rate of VAT on all commissions.
24. We have been involved in on-going discussions with HMRC and also significant clients, such as Santander and Allpay. Allpay's exemption was removed by HMRC and an appeal rejected. Santander continue to prefer exemption to be applied to our services, but are prepared to accept VAT being levied.
25. In October, after review by Santander, we sent a letter to HMRC seeking the maintenance of the VAT exemption. We believe HMRC will reject this approach. We await a response.
26. Additionally when we acquired Payzone in October 2018 it was confirmed that its business operations were structured in a very similar manner to that of PayPoint, which would be highly likely to lead to HMRC arguing that VAT was applicable to its post bill payment

Confidential

4



services. For Post Office group of companies it would not be practical to have a single service being treated differently for VAT purposes for POL and Payzone.

27. Although there are a number of complexities in this area, a review of the impact of applying a standard rate on all commissions showed that it would benefit POL by approx. IRRELEVANT of additional VAT recovery per annum because of the partial exemption method that we use. This would be a recurring benefit driven by a higher VAT recovery rate.

What progress has been made around the changes to the tax team described in the last update?

28. HMRC's have previously indicated that, based on the size and complexity of the business, POL's tax team was under-resourced. In April 2019 we recruited a second full-time team member to support the tax manager particularly in the corporation tax area.
29. We continue to take specialist advice where appropriate, notably from KPMG and Deloitte.

6

What other tax related issues should the ARC be made aware of?

Governance and Tax controls

30. HMRC's governance report from 2016 is being updated and we expect it to be issued in February 2020. The 2016 report highlighted a lack of documented process around tax and tax risks reporting. In intervening period new procedures, which have had HMRC oversight, have been introduced to embed tax policy and understanding of tax risk in the business.
31. The tax controls developed are reported monthly through PwC's 'TrAction' tool with supporting documentation provided. Quarterly Tax issues reports are circulated to senior staff, including the CFO, Head of Legal Services and the Group HR Director.
32. New process guides have been written documenting all VAT return processes and supporting review guides to evidence that checks have been carried out. A new VAT reconciliation process had been developed and new general ledger accounts created to provide a clearer audit trail. These processes have brought about the identification of the historical errors highlighted above.
33. HMRC have confirmed during their VAT reviews over the last 18 months they are satisfied with the improvements and controls made by the tax team.

HMRC Business Risk Review +

34. In late 2019 HMRC introduced its new, business tax rating regime. HMRC has set out more guidance and shared expected standards in order to achieve each rating category. POL group was rated 'non-low risk' in 2018. It is expected that this rating will continue, albeit being rebadged as 'moderate'. This is mainly due to our size and complexity, although over time the Tax team's aim is for POL to be rated to low risk through further automation, checking, controls and education.

HMRC VAT Audit

35. Phase 2 of HMRC's audit to examine accounts receivable processes was completed in June 2019. They were satisfied with the information presented and the integrity of reporting. HMRC are continuing to carry out audits across different areas of tax processes.



Making Tax Digital

36. Making Tax Digital is a key part of the government's strategy to make it easier for individuals and businesses to get their tax right and keep on top of their affairs. HMRC's stated ambition is to become one of the most 'digitally advanced tax administrations in the world, modernising the tax system to make it more effective, efficient and to ease compliance'. The initial phase, started on 1 October 2019 for POL. This introduced a mandatory requirement to upload VAT return information digitally to HMRC's new portal.
37. POL purchased software from PWC to facilitate this process. We submitted our first MTD compliant VAT return in October 2019.
38. From 1 April 2020, with a 12-month "soft-landing" phase, there is an additional requirement to have information in the VAT returns 'digitally linked' before the transfer to HMRC. This aspect is more complex, requiring a review of POL's systems to establish their compliance with HMRC's requirements. A project has commenced by the tax team to determine POL's position and to make recommendations for the correct investment.
39. Based on the actions of tax authorities in other jurisdictions it is expected HMRC will require further business data to be shared via the portal in the future, with an expectation that supporting VAT return information, such as AP and AR data will be accessible by HMRC.
40. VAT is the first tax to be reported digitally to HMRC. Once HMRC is confident that the system provides the requisite data and ease of access for both taxpayers and HMRC further taxes will be required to be reported digitally. In 2019 HMRC announced a delay to the introduction of digital corporation tax reporting, which was due from April 2020, there is no official revised introduction date, but it has been confirmed to be not before April 2021.

6

Brexit

41. We do not anticipate a significant tax impact from Brexit as our business is predominantly UK based. There may, however, be an impact for some of our suppliers where they have cross border supply chains and work has been carried out by colleagues to gain reassurance in this area. This could lead to an increase in costs of procuring goods if Customs duty becomes due. It is likely that businesses would seek to pass on increased costs.

Tax Strategy – Annual Review

42. Following the approval of the draft POL Tax Strategy by ARC in November 2017 it was made available publicly on the website in January 2018, highlighted internally in ONE Focus and a copy sent to HMRC. The revised Strategy will be republished after approval.
43. HMRC requires an annual review and updates to a Tax strategy where appropriate. The Tax team has reviewed the Strategy and made minor amendments around dating of the document and legislative references based on HMRC's recommendations. This ensures it remains fit for purpose and reflects our position.
44. The revised Tax Strategy is set out in Appendix 1.



Appendix 1 – Post Office Group Tax Strategy

This publication sets out the tax strategy of Post Office Limited and its UK subsidiary undertakings (referred to hereafter as the "Group" or "Post Office") for the financial year 2020/21, and in making this strategy available the UK Group is fulfilling its responsibilities under the Finance Act 2016, Chapter 24, Schedule 19, Part 2, Paragraphs 16 & 17.

This tax strategy applies to UK taxes applicable to the Post Office and its affiliated entities both in the UK and overseas. The document is ultimately owned by the Board of Directors of Post Office Limited ("the Board").

The tax strategy is reviewed annually, updated as appropriate and approved by the Board each January to cover the next financial year. The Board, along with assistance from the Group Finance teams, take ultimate responsibility for setting, monitoring and amending the strategy as required.

6

In summary, the Post Office is committed to:

- following all applicable laws and regulations relating to its tax activities;
- continuing to have an open and honest relationship with HM Revenue & Customs driven by collaboration and integrity; and
- applying diligence and care in our tax management, and ensuring that our tax governance is appropriate.

How the Post Office manages its tax risks

The Group's on-going approach to UK tax risk management and governance is based on the principles of reasonable care and materiality. The Post Office maintains on-going application of tax governance, including frequent risk metric assessments and the review of applications of strong internal control procedures, in order to substantially reduce tax risk to materially acceptable levels.

As part of this governance, the Post Office has identified tax risks, which are maintained internally on risk registers, with their materiality being assessed based on a corporate risk matrix. The matrix then records the potential impact, subject to two contributory factors, the exposure if the tax risk crystallises and the relative likelihood of the risk crystallising.

A detailed log of these risk reviews is maintained monthly. A summary report is then presented with significant / material issues to the Chief Financial Officer for his consideration, further discussion at Board level and with HM Revenue & Customs should the issue merit engagement of the tax authorities. Where decisions are deemed to be complex, or have an element of uncertainty assistance from third parties may be sought to aid the Post Office's decision-making process.

Tax planning

Given that the Post Office is owned by the British Government's Department for Business, Energy & Industrial Strategy, it understands the importance of its transparent business operations.

Confidential

7



The Post Office will not engage in artificial transactions the sole purpose of which is to reduce UK tax. As well as the above the Post Office will not engage in tax efficiencies if the underlying commercial objectives do not support the Group's position, or if the arrangements impact upon the Post Office's reputation, brand, corporate and social responsibilities, or future working relationships with HM Revenue & Customs.

Approach towards dealings with HMRC

The Post Office have always been and remain committed to maintaining integrity and transparency when dealing with HMRC. The Post Office underlines these principles by agreeing to:

- Accurately disclose all information required in correspondence and returns, and efficiently respond to communications as and when required. Where additional work is required, such as in the event of a disagreement, we will look to resolve this in the most professional and efficient way possible.
- Be open and transparent about decision-making, governance and tax planning, firstly by ensuring that it is liaising directly with our dedicated HMRC team and secondly by publishing our tax strategy easily accessible within the public domain.
- Ensure all interactions with HMRC are conducted in an open, collaborative and professional manner.

6

Signed

Alisdair Cameron

Chief Financial Officer and Senior Accounting Officer

(Updated January 2020)



Post Office Limited Audit, Risk & Compliance Committee Report

Title:	Insurance Renewal 2019 – Ratification of Spend
Meeting Date:	28 January 2020
Author:	Mark Dixon, Head of Treasury, Tax & Insurance
Sponsor:	Alisdair Cameron, Chief Financial Officer

Input Sought

Action Required: Noting/ Decision	The ARC is asked to ratify the spend in connection with the 2019 Insurance Renewal.
Previous Governance Oversight:	

Executive Summary

Context:	As a follow up to the paper presented to the Audit, Risk and Compliance Committee in September 2019 and email exchange in December 2019 approving the spend, this paper sets out the final insurance renewal spend for 2019 and seeks formal ratification for that spend.
-----------------	---

Confidential



Report

1. The business has a series of insurance policies which were due for renewal on 1 November 2019.
2. At its meeting on 23 September 2019 the ARC approved the 2019 Insurance Renewal on the basis of a paper submitted by Mark Dixon. The amount approved by the ARC was **IRRELEVANT** (excluding IPT and the additional spend on Cyber to increase the limit from **IRRELEVANT** to **IRRELEVANT**).
3. At the meeting deteriorating conditions in the crime market and the uncertainty around final premium amounts were discussed. Unfortunately the market continued to be very tough and the final premiums settled on were higher than anticipated in September. The premium increases seen were a reflection of the market in general and are not specific to Post Office. It is believed that actions that the team has taken over the last couple of years to build relationships with insurers in this market have in fact helped mitigate the impacts to a degree.
4. In an email on 2 December 2020 members were asked to approve spend of up to **IRRELEVANT** (excluding IPT and the additional spend on Cyber to increase the limit from **IRRELEVANT** to **IRRELEVANT**). Approval was subsequently received for the higher spend level by email.
5. We are therefore seeking your formal approval to ratify the final spend for the 2019 Insurance Renewal which was **IRRELEVANT** (excluding IPT and the incremental Cyber) per the table below.
- 6.

	Premium 2019/20	Premium 2019/20	vs Last Year (£)	vs Last Year (%)	Comments
Crime *	<div>IRRELEVANT</div>				
Cyber (current limit)					
D&O					
Combined Liability					
Motor					
POL PI					
POMS PI					
PDBI					
Terrorism					
PA Travel					
Sub-total (excl additional Cyber)					
Cyber (increased limit)					
Total					
<i>All premiums exclude UK Insurance Premium Tax at 0%</i>					
<i>* Based on 1 month extension on existing terms and 11 months on renewal terms</i>					



Post Office Limited Audit, Risk & Compliance Committee Report

Title:	Strategic Portfolio Office Change Control Environment Update
Meeting Date:	28 January 2020
Author:	Dan Zinner, Chief Transformation Officer
Sponsor:	Nick Read, CEO

Input Sought:

Action Required: Noting	For noting
Previous Governance Oversight:	September 2019 ARC paper on "Transformation Office Changes"; November 2019 Investment Committee approved changes on ToR & reporting process

Executive Summary

Context:	Following on from ARC paper "Transformation Office Changes" paper dated 23 September, ARC has requested: <i>"A further update on the change control environment would be presented to the ARC in January 2020."</i> In the past 4 months, several changes have been identified and implemented, while at the same time the Change environment is embedding and implementing further changes to increase control, mitigate risk and manage change. This paper provides a high-level update and draws attention to the areas of needed improvement which are currently being worked on. No decisions are required.
-----------------	--



Questions asked & addressed

1. What specific controls are in place to manage and gain value for money in change spend?
2. What new controls have been identified and implemented since the last Change ARC update, and what are still to be implemented?
3. What is the role of the business in change ownership and accountability?

Report

What specific controls are in place to manage and gain value for money in change spend?

4. In terms of Finance controls, all CapEx and Exception spend (WBS codes) have limits set by central Strategic Portfolio Office (SPO) Governance in a central tracking database. Thus, no spend over approved limits can occur. The approved limits are feed daily to the central finance teams (Project MasterData Controller) to feed into SAP so that no invoices over approved spends can be automatically paid. In addition, reports are sent as spend levels come close to 100%. The SPO Governance team will not add additional spend until approved by the appropriate Governance Forum as set by the ToRs for each forum, including Board noting/approval for total spend over £5m.
5. While project teams indicate total project spend, Governance forums mostly approve spend in phases or tranches to limit overspend. Projects must come back through the appropriate Governance forum for additional funding (i.e., "draw down") to continue the project, which is not always guaranteed. In the past it was "assumed" by projects that they had their total budgets "ring-fenced" and this is no longer the case. Governance forums are also empowered to challenge spend requests and have granted less than project requests.
6. In addition, new project finance processes have been put in place that require all projects to re-forecast spend and benefits on a monthly basis only through Anaplan, as the one source of truth. This enables the SPO to continually re-prioritise and challenge project spend while ensuring that projects actively manage their spend and forecasts. Automatic links have been put in place between Anaplan and Service Now (SNOW, the central Change master database) to ensure only one forecast exists.
7. In terms of value for money, external contractors have commented that rates that POL pay for certain services are higher than observed for private sector companies. However, it is noted that the nature of the Post Office requires specific costs, e.g., historic IT contracts or OJEU requirements. Thus, it is difficult to compare with other private companies. Rather value for money measures should be viewed in terms of standard ROI measures. The FP&A team are working with Change to embed these into Anaplan to include this in future Portfolio metrics of success. However, some projects will not have an ROI, e.g., compliance or regulatory programmes, legal costs, etc.



What new controls have been identified and implemented since the last Change ARC update, and what are still to be implemented?

8. In September 2019, the Chief Transformation Officer set out a plan to upgrade the Change function. This was based on initial observations and the need to:
 - a. place capable and competent resources on appropriately configured on teams;
 - b. increase organisational clarity and accountability;
 - c. raise the quality of support and challenge earlier in the process;
 - d. increase the frequency of portfolio oversight with new routines, rhythms and reports to speed up issue identification;
 - e. broaden stakeholder understanding of, and conviction for, how 'Change works' at the Post Office to make the process more efficient, and;
 - f. assist with GE to role model and embed a consistent way of working to improve the quality of planning and control
 Progress against this plan, which was laid out in 3 focus areas (People; Process; Perception), has been described in **Appendix 1**.
9. In terms of controls, much progress has been made by the central SPO team to: highlight standards; actively manage and churn underperforming individuals; manage our contractors and costs; raise the quality of challenge in Governance forums; update ToRs and the Change Excellence Framework; and have one central repository (SNOW) for project information – a single source of truth.
10. In addition, the SPO now reports weekly and monthly on projects across a variety of measures (see reading room for examples). These reports give the SPO additional opportunities, as a control measure, to frequently review project data, data quality, progress and scope. The reports create a purpose to investigate specific projects in specific areas: finance, delivery, risk, etc. However, more work could be done to create triggers for additional ad-hoc non-gate reviews by Finance or IT to increase accountability for overspend or delays.
11. IA will highlight the improvement opportunities of current controls in their next review of Change; however, the CTO believes more work can be done to standardise Project Assurance. Currently, project assurance is completed in an ad-hoc manner based on opinions or requests. While this can continue to optimise our limited resources, the SPO are working on creating clear, internal triggers and tolerances for project assurance reviews (risk, health check, delivery assurance). Moreover, the SPO needs to work on identifying ways to institutionalise project "lessons learnt," given the amount of people change within the Post Office and the Change community. Post Implementation Reviews are codified and searchable but Change currently relies on institutional knowledge to highlight past lessons. A working draft of Change Assurance controls can be found in the reading room.
12. While more can be done to create additional controls, improvement is also needed in "people understanding": communications, training, induction, conviction for Change processes and governance. The significant work in creating the Change Excellence Framework needs to be leveraged. The CTO believes this will be a continual process to communicate to current and induct new POL colleagues. In addition, the new "Change



People” team will start using the developed Competency Framework to assess our current Change resources and continually raise the bar on resource quality.

13. It is the intent of the CTO to draw a line in the sand on the requirement for data quality and completeness in the Change community into the central SNOW repository by the end of the financial year. This target ensures that assurance and oversight can happen in an effective and efficient manner in FY20. To enable this, the SPO team need to complete standards, create assurance triggers, process changes to job descriptions for Portfolio PMOs (so that there is clear accountability) and create additional reporting mechanisms to monitor data quality and completeness. A reduced portfolio of projects will also assist to create focus.

What is the role of the business in change ownership and accountability?

14. The role and relationship of Change and the business (i.e., Finance, IT, commercial areas, etc) has not changed. At the moment the role of Change is to support the business in developing the method to deliver change objectives and then deliver according to the agreed plan. However, ownership and accountabilities are not universally understood or agreed. So, in line with the 3rd focus area of the CTO’s original plan (Perception), more focus is required on raising the level of ownership and accountability through: communication, standardisation, controls and behavioural changes.
15. Within Change, understanding of accountabilities and quality of assurance between the 1st and 2nd line also has room for improvement which is a result of the new roles within Change. This should also improve with time, especially as we reduce projects.

8

Stakeholder Implications

16. Given the Change function supports all areas of the business, continuous improvements in controls and actions to increase accountability understanding will affect all stakeholders. This continued focus will be in 2 groups: 1) the Change Community through training, weekly “drop in clinics”, performance management, quarterly “Town Hall” group sessions and monthly Q&A sessions); and 2) POL Senior Leaders through one on one direct interactions with Change leaders (SPO, CTO and Portfolio Leads). The SPO will continue to developed and communicate RACI’s, monitor and control incorrect accountabilities and role model appropriate ones.

Next Steps & Timelines

17. At the moment, the SPO is working with IA to define, develop and refine the current Change controls framework. Change continues to request support from IA to ensure Change controls are aligned with IT controls
18. At the same time, the CTO and SPO continue to improve controls identified in this paper and look forward to the February IA audit of Change to identify further areas of improvement.

4

Internal



Appendix 1

In September 2019, CTO's short term identified plan was to embed Change processes and ways of working through consistency, clarification and communication. The plan emphasised the immediate need to focus on the Change community first by increasing understanding on how to consistently manage and resource a project for delivery (and thus implicitly not focus on "strategy"). The plan sought to embed the former COO's original changes (centralised Change organisation and Change Excellence), while raising the quality of management and challenge and simplifying changes to further engage the overall business on Change. The plan includes a focus on People, Process and Perception.

The table below is the CTO's self-assessment of progress made so far. It notes that good progress has been made in the "Process" section, but much more is needed in the "Perception" section.

CTO FY19 Focus Areas	Progress to Date		Work to continue
People			
Structure fit for purpose Change teams		3 in SPO responsible for all skills pool resources (PM, PMO, BA)	Review all current project teams, starting with Gold/Plat, to ensure they are properly structured
Increase capable and affordable Change resources		50% contractors down from 62% YoY; 1 day contractor cost, down 56% YoY	After portfolio focus (post-PSG), move to more FTC affordable resources
Communicate value of the centralised Change support team		Full SPO team, clear JDs, communicated to Change & Business; structured PLs	Further consolidate Portfolios while demonstrating value of full SPO team
Process			
Operationalise Change routines and rhythms		2 monthly cycles of "Change heartbeat" focus areas with data in SNOW; weekly dashboards	Increase SNOW data quality and ad-hoc assurance reviews and triggers; additional dashboard context
Embed the Governance process and tools		Increased transparency, issue raising, and questioning of cases	Earlier interventions into projects to scope better and speed up governance process, link to strategy
Actively manage Change (resolving issues, making decisions, creating transparency and prioritising)		Monthly project forecasting and 3x/month cross-portfolio collaboration meetings to highlight Programme risks, dependencies	Stronger finance accountability earlier through increased Change collaboration; further dependencies identification
Perception			
Foster understanding, conviction and alignment on how POL "does Change"		Ad-hoc training on SNOW/Change; monthly Change community "All Hands" update sessions	More formalised training on Change Excellence for Skills Group resources
Bring management along on the overall change vision and journey		Ad-hoc reviews of change progress outside of IC	Leverage weekly and monthly reporting to bring GE/SLP closer into Change activity
Communicate the wider Change story		No progress so far	Part of wider PSG story, communication on Change ways of working to support PSG



Post Office Limited Audit, Risk & Compliance Committee Report

Title:	Money Laundering Reporting Officer Annual Report
Meeting Date:	28 January 2020
Author:	Sally Smith, Money Laundering Reporting Officer & Head of Financial Crime
Sponsor:	Ben Foat, General Counsel

Input Sought

Action Required: Discussion	To review the annual report and conclusions ensuring Post Office's compliance with its regulatory obligations under the Money Laundering Regulations, and endorse the recommendations.
Previous Governance Oversight:	N/A

Executive Summary

Context:	The Money Laundering Regulations (MLRs) require that the Money Laundering Reporting Officer (MLRO) produces an annual report to appraise senior management on the effectiveness of key Anti-Money Laundering and Counter Terrorist Financing (AML/CTF) controls, and make appropriate recommendations for improving the management of risks, priorities and resources, if appropriate.
-----------------	--

Questions asked & addressed

1. Is Post Office complying with the requirements of the regulation?
2. What are the key AML and CTF risks within Post Office Ltd and are there any significant gaps or weaknesses in the Post Office's compliance with its regulatory obligations under the Money Laundering Regulations (MLRs)?
3. What are the key activities that need to be undertaken to address these gaps

Report

4. The annual report is attached and covers the key reportable regulatory responsibilities under the MLRs. Appendices referred to in the report are in the reading room.

Financial Impact

5. Post Office have not received any regulatory penalties since 2017/2018 when HMRC fined us [IRRELEVANT] for regulatory breaches in relation to Travel Money. We have however seen increasing scrutiny by regulators in the UK, which seems to reflect the guidance in the Financial Action Taskforce Mutual Evaluation Review published at the end of 2018 and [IRRELEVANT] of fines have been levied by UK regulators in 2019. Additionally, HMRC annual registration fees have increased significantly from [IRRELEVANT] in 2018 to [IRRELEVANT] in 2019, which together with the cost of complying with Fit & Proper requirements and transaction monitoring and assurance, represents a significant cost to the business.

Risk Assessment, Mitigations & Legal Implications

6. Products and services provided by Post Office are broadly in line with the risk appetites set by the Board although there has been a significant increase in money laundering via the Banking Framework services. Other than these services there has been an improvement in residual risk over the last 12 months.

Conclusions & Recommendations

7. The regulatory environment continues to pose a challenge, with increased regulatory and legislative focus on money laundering and terrorist financing. Following the 2018 FATF UK Mutual Evaluation review, there is evidence of increasing focus by regulators, and readiness to exercise monetary penalties, as evidenced by the Office of Financial Sanctions Implementation (OFSI) and the FCA. We have also seen a more pro-active approach to supervision by HMRC (funded by the significant increase in registration fees from 1st May 2019) and an increase in the volume and scale of penalties issued by them. This indicates that should HMRC identify that Post Office has failed to comply with money laundering regulations, penalties will be more egregious than historically, as well as being made public. It is therefore important that Post Office's commitment to comply with all aspects of regulatory requirements remains high on the agenda. **Regular reporting by MLRO through RCC and ARC, and sponsorship of required actions by GE.**

8. The Supranational Risk Assessment issued on 2019 highlights that cash remains the number one choice for criminals to money launder, and this has been borne out by the increase in suspicious activity that has been identified through the year relating to Banking Framework cash deposits over Post Office counters
9. Political uncertainty delayed publication of the UK legislation relating to the Fifth Money Laundering Directive, but this was laid before Parliament on 20th December 2019 and implemented on 10th January 2020. The legislation is still under review, but Post Office impacts are limited:
 - Further emphasis has been placed on risk assessment – particularly prior to the implementation of new products, services or technology
 - Giftcard limits were reduced from £400 to £120 to meet the new regulations
 - The regulations have not specifically covered Politically Exposed Person, and the status for Post Office executives is being checked.

Full de-brief to be included in March RCC and ARC Compliance reports

10. The establishment of the National Economic Crime Centre (NECC) in October 2018, has seen an increased focus in activity, and this is borne out by the increased workloads we have seen responding to subject requests, which have doubled year on year. A number of the cases under review relate to cash-based criminal activity with a predominance in human trafficking, organised immigration crime, modern slavery and sexual exploitation.
11. The HMRC supervisor who has overseen Post Office regulated activity since 2015 is retiring in June 2020, and therefore Post Office will have a new supervisor during the early part of 2020, which may bring changes to HMRC regulatory oversight and activity. We are also aware that HMRC are considering a further review of their registration fee structure, although as yet, there has been no guidance on this.
12. Further work has been undertaken to resolve data issues with the Bureau de Change monitoring solution and assessment and oversight of the product continues to mature. The increased volumes of investigations and SARs evidences the improvement in controls since the HMRC audit in 2016 and subsequent penalties. The new premises registration reporting tool was delivered by DCoE in 2019 and has improved the accuracy of registration data. However, more work is required to generate the HMRC reports in the correct format and remove manual manipulation. Customer Due Diligence, PEPS and Sanctions checks for Bureau de Change are currently assessed to be adequate.
13. The agent Fit & Proper data requirements have continued to be a significant challenge for Post Office, and data gaps and challenges in providing accurate monthly reporting to HMRC remain due to the disparate systems that store the information. Significant effort was required to meet the extended deadline of September to complete the data submission to HMRC, although ultimately only 85 premises were deregistered, albeit further data discrepancies were then identified. Data integrity issues have continued and until the new data system is designed, built and delivered (scheduled for April 2020) this will cause ongoing issues that put Post Office at risk of regulatory scrutiny. Additionally, due to the high number of structural changes within Post Office over the last 12 months, it has proven difficult to keep the direct employee Fit & Proper tests up to date with HMRC, and the

business is giving insufficient review of regulatory oversight responsibilities when changing reporting lines and/or roles, which must be addressed moving forward.

Meetings have been set up between the MLRO and HR to tighten controls

14. Following increasing workloads over the previous two years, two additional financial crime roles were created and recruited into Financial Crime Compliance during 2019, and this has ensured that enhancements could be made to Bureau de Change transaction monitoring and investigation, the back log of risk assessment work brought up to date and more focus given to industry and regulatory horizon scanning to ensure that Post Office is adequately protected. The team has also absorbed the continued increase in investigations (up 40% compared to 2018) and SARs (up 35% compared to 2018), although if this trend continues, this will not be sustainable. There is limited, if any, automation that can be introduced to cover these tasks.
Workloads and resourcing implications will be monitored by the MLRO during 2020
15. The Bureau de Change residual risk continues to improve as increased controls and improvements to transaction monitoring are implemented. Risk Assessments for Post Office Insurance have fallen behind due to product managers failing to complete Product Information Packs/respond to queries in a timely manner and this has been highlighted to the POMS ARC. First line compliance with Post Office financial crime policies is of concern. **Further work will be undertaken by Compliance in 2020 to improve first line management awareness of the policy minimum control requirements that are their responsibility.**
16. Work has commenced to undertake assurance activity in respect of Payzone products and services. There is currently a lack of documented policies and procedures to support this area of the business, but it is planned that the initial assessment and assurance activity will be concluded by the 2019/20 financial year end.
17. There have been a number of high value and high profile investigation cases relating to money laundered through Post Office counters via accounts held by banks operating within the Banking Framework. This has resulted in significant interest and focus by various law enforcement organisations culminating in the establishment of Project Admiralty by the NECC with key stakeholders to address the risks and issues. Up to P8 2019/20, there have been investigations and SARs relating to c.92m of cash deposits. **The business, particularly Product Management, must ensure that adequate focus and support is given to industry, NECC and Post Office initiatives to address the migration of cash placement risks to Post Office as banks close, including following through on the actions recommended in the Banking Framework risk assessment.**
18. Overall, there has been a significant improvement to mandatory training compliance in the Network, brought about by the roll out of SmartID and training controls. Training and awareness remains a key control for AML/CTF and challenges remain:
 - Whilst all Horizon users now complete the training and test, it is evident from branch visits by Compliance that the key messages are not landing, and branches are sometimes failing to question transactions or report suspicions, either because they lack confidence, or because they do not understand how to apply the training.

With the current method of delivery of training via Horizon, there is limited scope to improve the content.

- **Compliance will continue to work with the Area Management team and the NFSP to identify different ways to deliver key messages.**
 - **Compliance are looking to design and deliver animations as part of the annual AML/CTF training in May to help land key messages, but as these cannot be incorporated into Horizon, alternative access will be investigated for the Network.**
 - There are still challenges with back office staff completing training within the required deadlines. **Financial Crime Compliance will continue to monitor and chase.**
19. In summary, the framework of AML/CTF controls is generally effective and Post Office is meeting its regulatory requirements under the MLRs. However, there are key areas where focus needs to be maintained to ensure this continues, particularly in relation to:
- The completion, maintenance and timely and accurate provision to HMRC of agent Fit & Proper data, and ensuring that HMRC direct employee checks are kept up to date
 - The substantial increase in suspicious activity relating to Banking Framework cash deposits
 - Increasing regulatory scrutiny and penalties
20. Additionally, attention needs to be given to ensure that:
- Key training messages have been understood and are acted upon by Horizon users and given the limitations of providing training over Horizon, alternative methods will need to be identified
 - First line are aware of their responsibilities to maintain policy minimum control standards
 - Increasing workloads from core regulatory activity (Bureau de Change transaction monitoring, SARs and investigations) can be maintained.

Key Recommendations:

Activity	Responsibility	Completion date
Continual focus on first line accountabilities e.g. policy minimum control standards, ensuring product and service risk assessment, integrity of F&P data and records	All Senior Management	Ongoing
Review 5MLD impacts	MLRO	End Jan 20*
Completion of premises registration reports	DCE	End March 20
Delivery of F&P data system to reduce errors	F&P Project Team	End April 20
Implement F&P assurance across impacted business areas	Compliance	Q1 2020/21
Raise awareness of policy requirements to first line	Business Senior Management & Compliance	Throughout 2020

Tab 9 Money Laundering Reporting Officer (MLRO) Annual Report

Initial financial crime assessment of Payzone	Compliance	End March 20
Initial implementation of financial crime controls in Payzone	Product	End March 20
Reduction of laundering risks in Banking Framework via work with NECC, Banking Framework partners, and law enforcement	Product & MLRO	Throughout 2020
Product to produce initial proposals to provide Compliance with improved MI to ensure appropriate balance of commercial considerations against regulatory risks	Product & Compliance	Q1 2020/21
Enhance AML training and awareness	MLRO, L&D, Network	June 2020

The Annual Report of the Money Laundering Reporting Officer for the Post Office Limited for the period 1st January 2019 – 31st December 2019

Table of Contents

A.	Purpose and Scope of Report
B.	Background
C.	Governance Framework
D.	Operation and Effectiveness of the Control Framework
i.	Senior management oversight
ii.	Staff awareness and training
iii.	Risk assessment, policies, controls and procedures
iv.	New products and services
v.	High risk products and services
vi.	Customer due diligence requirements
vii.	Reporting suspicious activity
viii.	Record keeping
ix.	Premises Registration
x.	Fit & Proper tests
E.	Incidents and Investigations
F.	External Threats/Landscape
i.	Business areas
ii.	The 4 th Money Laundering Directive
iii.	The 5 th Money Laundering Directive
iv.	The Criminal Finances Act 2017
v.	The Policing and Crime Act 2017
vi.	Joint Money Laundering Intelligence Taskforce
G.	Conclusions and Recommendations
	Appendix A: Post Office Insurance annual MLRO report
	Appendix B: Product and Service Risk Assessment Summary
	Appendix C: Summary of UK Enforcement Action
	Appendix D: Product and Service Risk Exceptions
	Appendix E: Report on duties of Nominated Officer – Suspicious Activity Report Summary

A. Purpose and Scope of Report

1. The Money Laundering Regulations (MLRs) require that the Money Laundering Reporting Officer (MLRO) produces an annual report to appraise senior management on the effectiveness of key Anti-Money Laundering and Counter Terrorist Financing (AML/CTF) controls, and make appropriate recommendations for improving the management of risks and priorities, and resources if appropriate.
2. HMRC is the regulator responsible for supervising Post Office Limited compliance with MLR requirements. Their oversight relates to Post Office Limited Money Service Business (MSB) activity, specifically, the provision of Bureau de Change.

3. The MLRs and the 2017 National Risk Assessment clearly identify a requirement for organisations to adopt a risk-based approach to prevent money laundering and terrorist financing. Risk assessment must be documented and evidence the decisions that senior management have made in the context of the particular risks facing the business.
4. The Post Office Insurance business is subject to a separate MLRO annual report in September each year, and can be found in Appendix A.

B. Background

5. The MLRO and the Financial Crime Compliance team are responsible for financial crime policies, assurance and AML/CTF risk assessment of products and services (see Section D and Appendix B).
6. Bureau de Change is the only product that Post Office is directly regulated for, although POL is required, both contractually and under the MLRs, to have in place and comply with policies, controls and procedures to mitigate and manage effectively the risks of money laundering and terrorist financing for all the products and services it offers through third party or white label solutions and joint venture arrangements (e.g. MoneyGram, Banking Framework Services, Post Office Money products, Gift Cards etc.). The most significant impact of financial crime for Post Office continues to be reputational damage. Negative media attention following an incident of financial crime has potential for loss of consumer and client confidence in the product/service, consequential devaluation of brand values and possible impact on Government commitment which is vital to support Post Office.
7. Post Office have not received any regulatory penalties since 2017/2018 when HMRC fined us [IRRELEVANT] in respect of premises registration errors, and [IRRELEVANT] for regulatory breaches in relation to oversight and risk assessment of Travel Money (this latter fine being halved due to co-operation and progress during the audit). We have however seen increasing scrutiny by regulators in the UK, which seems to reflect the guidance in the Financial Action Taskforce Mutual Evaluation Review published at the end of 2018 and [IRRELEVANT] of fines have been levied on firms by UK regulators in 2019. (see Appendix C for summary of UK enforcement action)
8. Training and awareness continues to be a key control for Post Office and the introduction of training controls with Smart ID has ensured all Horizon users complete annual training. There continues to be evidence however, that the key training messages are not being applied consistently (see para 23)
9. The new requirements relating to Fit & Proper tests for agents under the 2017 MLRs have required extensive work, and Post Office was granted a 3 month extension by HMRC to complete the agent data gathering exercise. Work to complete this and implement BAU processes continues to be an area of focus (see paras 60-61).

C. Governance - those responsible for anti-money laundering systems and controls, and the structure within which they operate

10. Ben Foat is the GE member and officer appointed to be responsible for overseeing compliance with the MLRs.
11. Sally Smith is both the MLRO and a member of the Post Office Compliance leadership team. She is located in Finsbury Dials, Moorgate, London, where Post Office Group is situated. The MLRO takes ultimate responsibility for compliance with the MLRs, the provision of training and awareness within Post Office, the design and implementation of internal anti-money laundering policy, systems and procedures, and advising on how to proceed once an internal report and/or Suspicious Activity Report (SAR) has been made
12. Under the direction of the MLRO, Compliance is responsible for assessing and assuring Post Office Limited's exposure to financial crime. This includes
 - setting policies and standards relating to financial crime, assessing and assuring AML/CTF risks across Post Office;
 - ensuring that risks are properly reflected in Risk & Controls Matrices (RACMs);
 - ensuring appropriate disclosure of SARs to the National Crime Agency (NCA);
 - liaising with third parties regarding investigations; and
 - ensuring information is appropriately disclosed to clients or third parties.
13. Through the Financial Crime Compliance team, the MLRO has oversight of AML/CTF investigations, non-conformance by branches or individuals and risk assessment of products and services at a granular level.
14. During 2019 regular reports have been provided to the Risk & Compliance Committee (RCC) and the Audit, Risk & Compliance Committee (ARC) covering AML/CTF controls, the outcomes of risk assessment work, HMRC supervisory activity, changes to legislation and industry issues.
15. Due to increasing regulatory supervision and workloads two additional financial crime roles were created and recruited at the beginning of the 2019/20 financial year. This has ensured that a backlog of risk assessment work has been brought up to date, and enhanced Bureau de Change transaction monitoring and suspicious activity investigation capability has been implemented.
16. Other than for Bureau de Change, financial crime MI reporting within Post Office is still not sufficiently granular at product level to aid transparency and decision making. Product specific monthly MI on the work undertaken by Financial Crime Compliance is being developed and shared with the relevant product teams, with monthly MI currently provided to the Travel Money Product Director. Consistency of information and analysis capability for other products and services (especially Banking Framework) makes it harder to appropriately balance commercial considerations against regulatory risks. Compliance will work with business teams to provide Compliance with improved MI, with the aim of producing initial proposals by Q1 2020/21.

D. Operation and Effectiveness of Control Framework

i. Senior management oversight

17. See Section C above for summary of governance and oversight.
18. HMRC fit and Proper tests must be performed on all external Board Directors, GE, the MLRO and impacted employee roles as per HMRC requirements and Post Office policy.
19. However, recent structural changes across the business have been implemented without being effectively impact assessed to ensure that appropriate tests are completed for those roles overseeing regulated activity, and removed from HMRC records where individuals move to non-designated roles or leaving the business.

ii. Staff awareness and training

20. Provision of staff awareness and training is a key control for Post Office, and annual training was updated to cover issues and incidents that had arisen in the previous 12 months. All staff are required to complete AML/CTF training:
 - For back office staff this must be completed within 30 days of joining and annually
 - For customer facing staff this must be completed before they have access to Horizon and annually
21. Monitoring of training completion levels for back office staff is undertaken by HR Directors, and those staff who do not complete mandatory compliance training are dealt with via conduct with potential removal of annual bonus payment. Training completion is subject to quarterly assurance checks by Compliance. During 2019, there have been a number of times when functional areas have been chased as completion rates have been below 95%.
22. Annual training was completed between 3rd and 29th May 2019. Training for Horizon users was the first compliance module to be completed after the full roll out of SmartID and training controls and at 7pm on 28th May 2019, 74% of branches were fully compliant, and 88.3% of individuals. We therefore extended the Horizon user deadline until 3rd June 2019, by which time 93% of all users were compliant. By the 5th June, 92.4% of branches were fully compliant and 97% of individuals.
23. The number of failed test attempts, and low volume of SARs received continues to be of concern. Although SARs volumes are up year on year, a number of recent investigations have highlighted that SARs are not being submitted by Horizon users, and therefore key messages in the training are not being understood and/or acted on and work will be undertaken in 2020 to enhance awareness.
24. Following a number of high value banking deposit cases, the Financial Crime Compliance team, accompanied by two Area Managers, a Security Operations Manager and the London NFSP Executive member visited c.50 East London branches on Friday 25th October 2019 to raise awareness of criminal activity and the importance of raising SARs. Key learnings from these visits will inform further training and awareness across the network on AML issues. We are working with the Area Managers and NFSP to identify communication and awareness opportunities and developing animations to accompany the 2020 annual training which can also be used throughout the year to reinforce key messages.

25. 51 branch and business awareness communications on AML, Financial Crime and SAR reporting have been delivered in 2019. Over the last 12 months, we have tried to link communications to media reports of modern slavery, human trafficking and county lines drug dealing to try and help individuals to understand the link between criminal activity and their responsibilities.

iii. Risk assessment, policies, controls and procedures

26. The Group takes its legal and regulatory responsibilities seriously and consequently has¹
- **Tolerant risk appetite** for Legal and Regulatory risk in those limited circumstances where there are significant conflicting imperatives between conformance and commercial practicality
 - **Averse risk appetite** for litigation in relation to high profile cases/issues
 - **Averse risk appetite** for litigation in relation to Financial Services matters
 - **Averse risk appetite** for not complying with law and regulations or deviation from business' conduct standards for financial crime to occur within any part of the organisation
 - **Averse risk appetite** in relation to unethical behaviour by our staff.
27. The Group acknowledges however that in certain scenarios even after extensive controls have been implemented a product or transaction may still sit outside the agreed Risk Appetite. During 2019, there were 4 risk exceptions relating to financial crime. Three remain open but are relatively low risk and on track to close in 2020 (*see Appendix D for details*).
28. Product and service risk assessment has continued throughout 2019 with all new products and services assessed before go live. The new resource appointed in June 2019 has helped clear the backlog of assessments and improvements are being made to make this process more efficient and effective. (*see Appendix B for details*).
29. Product risk assessments for Post Office Insurance have been delayed in 2019, due to non-completion of the Product Information Packs by product managers. Additionally a new product (Gadget Insurance) did not follow the normal approval process, and therefore was not risk assessed before it went live in accordance with Post Office policy. These issues were reported to the Post Office Insurance ARC via their separate MLRO report in September 2019. Of 8 Post Office Insurance products, 6 have been assessed and 2 (Bike and Pet insurance) remain to be assessed and are overdue.
30. Policies relating to Financial Crime overall and AML/CTF specifically, have been updated and were approved at the September 2019 Audit and Risk Committee, and published on the Intranet via a One Communication.
31. Both first and second line management have responsibility to ensure that the controls in place work as intended, and the Financial Crime team undertake quarterly assurance checks against the minimum control standards. During 2020,

¹ The Risk appetite was agreed by the Post Office Board January 2015

further work will be undertaken to enhance this activity and provide enhanced assurance to Post Office senior management and Board.

32. We review, investigate and report all instances of non-conformance with AML policies and processes, ensuring corrective action is taken by relevant business owners.
33. Processes within Compliance are robust and up to date, however processes and policies across the business to support these are less mature and continue to require improvement.

iv. Development of new products

34. All new products and services have been subject to financial crime risk assessment. Following the acquisition of Payzone in October 2018, a Master Services Agreement between Post Office and Payzone has now been agreed, and a financial crime compliance review has commenced with a data gathering exercise. A number of key policies and processes do not appear to have been documented or implemented, but the assessment and action plan is expected to be drafted before the end of the 2019/20 financial year.
35. The Banking team is exploring cash automation and self-service devices. Compliance has supported the project and liaised with key banking stakeholders to identify potential risks and control requirements. The Banking team are looking to pilot self-service devices at 4 Post Office locations early 2020.
36. Compliance has supported the Retailer Point of Sale (RPoS) project which enables Postmasters to sell a selected range of Post Office products on their retail terminal. This service is currently deployed at 3 pilot locations with mobile phone top-ups, bill payments and Camelot products. In 2019, there was a change in strategy and the proposition is now also aimed at non-Post Office locations and work is ongoing with the project team to identify any financial crime risks and implement effective controls, as these locations will not have access to Horizon Online Help or any Horizon communications.
37. There have been no significant products or services launched during 2019 which have changed the regulatory risk landscape for Post Office.

v. High risk products and services

38. Post Office branch pre-order and on-demand Bureau de Change represents the highest direct risk for Post Office in terms of AML/CTF and regulatory compliance. Oversight and monitoring enhancements in 2019 include:
 - The use of Dynamics case management by Financial Crime Compliance has been further matured over the last 12 months and has supported more granular operational MI. This has enabled monthly MI Dashboard on monitoring, investigation and SAR activity to be provided to the Travel team.
 - A Business Objects specialist reviewed and tested the initial monitoring reports that were created. Improvements were made to speed up and streamline reports to improve efficiency.
 - In branch (on demand and pre order) Terms and Conditions have been approved and published on the Internet by the Travel Money Team, enabling Financial

Crime Compliance to write directly to customers who breach the £10k over 90 days threshold.

39. The Bureau de Change Credence universe has not yet delivered all of the functionality required. Accenture has rectified the majority of outstanding issues which were identified on delivery in June 2018 and these have been tested and put into production by the Data Centre of Excellence team (DCoE). There is still an outstanding issue relating to Sanctions whereby customer information is not being pulled through into AML Credence for on-demand transactions that decline due to a Sanction match. It was understood that this was going to be resolved as part of the fixes that Accenture have delivered, however, the DCoE team who were managing these changes did not raise this issue as they believed it had already been resolved. As the customer information is not showing on AML Credence, an interim process has been agreed with DCoE that they will provide the missing information when a match is identified. A Change Request has been raised with Accenture to resolve the issue. It should be noted however, that, as reported in 2018, the Credence universe and Business Objects solution delivered is not a transaction monitoring tool, and each report type has to be run and worked separately, which can cause customer or branch review duplication.
40. Other products that are high risk include:
 - Banking cash deposits – We have seen a rise in cash deposits from Partner Banks via Post Office counters as more customers become aware of the services and more bank branches close. All banks have implemented tighter controls around cash deposits and particularly via third parties and we have seen a migration of suspected money laundering of cash via our branches, a number of which have been undertaken by third parties and money-mules. Over the last 12 months there has been a significant rise in investigations and SARs relating to cash deposit services (*see para 67*).
 - Due to the rise in concerns about cash laundering via the Banking Framework Services (BFS), Post Office sought legal advice from Pinsent Mason regarding Post Office's regulatory position under the BFS agreement. They advised that although the Partner Bank has regulatory responsibility for conducting Know Your Customer (KYC) checks and transaction monitoring, the migration of cash deposits to Post Office represents a material risk terms of:
 - Potential regulatory scrutiny of Post Office and the partner banks, whether that is HMRC, FCA or other; and
 - Material reputational risk to Post Office brand if any action is taken by regulators or any criminal proceedings are brought for breach of the MLRs. If it is reported that Post Office has facilitated money laundering or terrorist financing, this level of negative publicity or regulatory scrutiny would be severe to Post Office given its social purpose within the UK communities and being solely owned by the Government.
 - In August 2019 the UK Financial Intelligence Unit (UKFIU) conducted a review of cash deposits via Post Office, calling out the increase in the number of SARs received by the NCA, the increase in banking services at Post Office providing criminals with more opportunities to place the proceeds of crime into the

financial system, and the lack of visibility Post Office has over the Partner Bank's customer meaning that SARs lack detail that would assist Law Enforcement. The UKFIU notes that there are clear indications of money laundering at some Post Office branches through the cash deposit services provided under the Banking Framework Services agreement.

- In July/August 2019, we identified 2 cases totalling c.£22m and HMRC presented these cases to the Joint Money Laundering Intelligence Taskforce (JMLIT), highlighting evidence that cash derived from criminal activity is being placed over Post Office counters. This appears to be highly organised crime using money mules and couriers, with funds deposited being immediately transferred to crypto currency. Following these cases and discussions between the MLRO and the NECC and the Pro-Active Taskforce of the Economic Crime Directorate at City of London Police, Project Admiralty has been established by the Operational Planning Coordination and Development (OPCD) team within the NECC and a working group has been established with the aim of obtaining a full and rounded picture of the threat from the banks in the banking agreement, the extent of their exposure, and the degree of involvement in any operational deployments.
- The first meeting was held on 23rd October 2019 attended by representatives from Barclays, RBS, HSBC, Santander, Lloyds, Post Office, HMRC, the Pro-Active Taskforce at the Economic Crime Directorate and members of the NECC. The aims of the project. Attendees were asked to produce more granular information from their systems but all banks stated that the funds identified in Post Office SARs relating to the large scale cases are generally immediately transferred to crypto-currency, and some to FinTechs. The crime groups identified to date have been African and Asian.
- Following the initial meeting, the Financial Crime team hosted bank representatives in the Post Office Model Office to demonstrate how banking transactions are processed and the challenges the Post Office faces. A further Project Admiralty meeting took place on 6th December at which bank representatives shared findings from their internal review, however, some were experiencing data mining issues and were unable to provide sufficient granularity. Some banks raised concerns about inter-bank sharing of customer data and each bank has been asked to evaluate their position and provide an update at the next meeting on 29th January.
- Analysis completed by the NECC relating to SARs submitted, containing the term 'Post Office' and 'cash', has identified a steady increase since January 2019. In October 2019, there were c.160% more SARs submitted when compared to January 2019, clearly indicating that banks and Post Office are identifying more instances of money laundering over Post Office counters. The NECC are continuing to monitor this and will update Post Office accordingly.
- The Financial Crime Risk Assessment of the BFS was completed and issued to the Banking team in November 2019 and has identified that there are control gaps exposing Post Office to regulatory, financial and reputational risks. An

action plan will be formulated to ensure that there are appropriate policies and procedures in place (in either Post Office or the banks) to enable Post Office to mitigate this risk and be able to demonstrate a robust response to any legal or regulatory action. The Banking team is setting up a working group and steering group to drive required actions.

- In addition to the work of the NECC and JMLIT, Compliance has briefed all the BFS banks on the current issues via the SCGC, and it has been agreed to set up a working group with appropriate representatives from the banks in January 2020 to help mitigate the risks.
- MoneyGram – As a near real time money transmission service, MoneyGram remains high risk for laundering and scams and there is significant training and awareness activity to help front line staff identify issues. In 2018, the US Department of Justice (DOJ) agreed to extend a Deferred Prosecution Agreement (DPA) against MoneyGram International Inc. due to significant weaknesses in their anti-fraud and anti-money laundering programme in 2012. As a result of this MoneyGram have implemented further controls to detect and prevent fraud over Post Office locations, which will ensure no Post Office location is in breach of their DPA.
- Gift Cards – Due to the anonymous nature of the product, we continue to see criminal activity which is addressed through training and awareness activity. There are planned product changes due in January 2020 to comply with the Fifth Money Laundering Directive, please refer to section 74.
- National Lottery & Scratchcards – Whilst these products could be used for money laundering purposes, this is seen as unlikely as it relies on obtaining a winning ticket. A key risk is failure in duty of care to customers if the product is purchased by vulnerable customers, or large volumes are purchased by an individual which may constitute excessive play. In 2019, the £10 scratchcard was withdrawn and there have been communications to the Network regarding vulnerable customers. This issue will be re-visited as part of the action plan to address the annual risk assessment by the Financial Crime team, which has been issued to the product team to assess materiality and propose any remedial actions. A meeting with the product team is planned for January 2020. Additionally, gaps in stock reconciliation for activated and non-activated scratchcards which could lead to theft or loss have been identified and escalated to the product team.

vi. Customer due diligence

41. Post Office Limited is required to undertake customer due diligence for directly regulated activity (e.g. Bureau de Change) when:
 - Establishing a business relationship, or
 - Carrying out an occasional transaction with a customer of €15,000 or more, or
 - Money laundering or terrorist financing is suspected
42. For Bureau de Change, the following controls are in place:
 - Horizon restricts single or multiple transactions in the same basket to £10,000 (well below the €15,000 occasional transaction limit).

- Staff training and Horizon prompts advise that no business transactions should be undertaken and that customers should not transact more than £10,000 in any 90 day period.
 - Customer details and ID are taken for all transactions of £1,000 and above, and for all transactions settled by card payment. Monitoring is undertaken to identify linked transactions for the same customer in a 90 day period and corrective action is taken as required. (See para 65 re. Bureau de Change investigations)
 - As part of Post Office's risk based approach, all transactions of £2000 and over are subject to a real time eKYC, PEPs and Sanctions check, with real time declines of eKYC failures and Sanctions matches.
 - Staff are trained to decline transactions and complete a SAR if they suspect money laundering or terrorist financing.
43. PEP matches are monitored post transaction with corrective action taken if necessary. In January 2019, a confirmed match was identified for an MP who purchased c.15k Euros from the House of Commons Post Office. This was raised to the MLRO and the branch were informed to advise all customers of the £10k over 90 day threshold particularly for transactions over £5k. No further issues have been identified.
44. For over £2k transactions, where there is a potential match on a Sanction list the transaction will be declined in real time. Over the last year, there have been 5 potential sanctions matches which have resulted in further investigation. Following review, none of these potential matches are the actual sanctioned individuals and therefore not reported to the Office of Financial Sanctions Implementation (OFSI).
45. From April 2019 to P8 YTD, we have prevented 24 customers from breaching the £10k over 90 day Bureau de Change threshold through monitoring activity, totalling £138,200.
46. For all other products and services, Post Office Limited is not directly responsible for customer due diligence, however, there are some contractual obligations where Post Office undertakes part of customer due diligence on behalf of the third party client or supplier. For example, where Post Office acts as agent for MoneyGram, we must comply with their policies and processes in relation to recording customer data and identification details. As part of product and service risk assessment work undertaken for these products and services, the requirement for customer due diligence, PEPs and Sanctions checks is considered, and where appropriate, work is undertaken with the product manager to ensure the right controls are in place.

vii. Reporting suspicious activity

47. All SARs are reviewed and, where appropriate, disclosed by Financial Crime Compliance under oversight by the MLRO. SARs received relating to third party clients are shared with them so that they can conduct an investigation against their own KYC and transaction records.
48. We continue to see more instances of Cash & Valuables in Transit (CViT) drivers raising SARs in 2019 due to the volume of cash they are collecting, and by Cash Centres in relation to Scottish & Irish notes, and in 2019 we have developed a specific SAR form to aid Supply Chain staff to report suspicious activity.

49. When reviewing network SARs, the team analyse the reports to determine whether to communicate the highlighted concerns to the targeted areas or the entire network (e.g. high value deposits, scams for vulnerable customers, customers transacting Bureau at multiple branches).
50. Overall the volume of SARs received is up from on average 240 per month in 2018/19 to 326 per month in 2019/20. This is an increase of c.35% and is mainly as a result of SARs identified from the new Bureau de Change monitoring reports. *See Appendix E: Report on duties of nominated officer for additional information*
51. An additional Financial Crime Manager achieved accredited Financial Investigator Officer (FIO) status during the year. Under s.378 of the Proceeds of Crime Act 2002, an FIO may exercise powers under the Act, and more specifically can receive SARs which have been disclosed to the NCA by reporters other than Post Office, where a subject has a potential connection with Post Office. There are now 2 accredited FIO's within Financial Crime Compliance and there has been an increase in review, investigation and response with 67 SARs disclosed by the NCA, in comparison to 34 in 2018.

viii. Record keeping

52. All record keeping relating to AML/CTF is electronic (all paper SARs and paperwork are scanned and saved electronically) and filed within a restricted access folders.
53. All reports, risk assessments and supporting documents are filed in the AML Sharepoint site, and a log is maintained to ensure annual review and sign-off.
54. For Bureau de Change, the new AML Credence universe maintains all branch on-demand and pre-order Bureau de Change transactions and this is retained for 5 years
55. Financial Crime Compliance investigation cases are managed and recorded via Microsoft Dynamics and maintained confidentially from other Dynamics users in the Post Office.
56. Court Orders & Data Protection Act requests – In 2019, we provided 1 witness statement to the Police and received 15 Data Protection Act requests from Law Enforcement and regulatory bodies relating to fraud and money laundering. 4 of the 15 Data Protection requests received were raised due to investigations highlighted and carried out by the team. In 2018, there were 7 Data Protection Act request and 4 witness statements.

ix. Premises Registration

57. During 2019, new reporting was built, tested and delivered by the DCoE for fortnightly submission of data to HMRC for premises registration. Data to generate the HMRC reports is now taken from the source Master Data Management system and this has removed previous reporting errors. Currently the data is manually transferred into the HMRC reporting templates, but we have discussed some data changes with HMRC and DCoE are expected to deliver reporting in the correct HMRC format early 2020, removing the need for manual work.
58. On 4th April 2019 HMRC increased branch registration fees from IRRELEVANT per annum with effect from 1st May 2019 meaning our annual registration fee for 1st

June 2019 was [IRRELEVANT], reflecting the [IRRELEVANT] increase and leaving no time for Post Office to consider the option of removing the service from branches to reduce the financial impact. Corporate Affairs engaged with BEIS, HMT & HMRC, but no extension could be accommodated, and the fee was paid in full. As part of the fee increase the HMRC Fit & Proper test fee for direct employees and Board members also increased from [IRRELEVANT], although this is still a one-off fee. Corporate Affairs has since been approached by HMT as it wishes to undertake a further fee review and has indicated that it wants to meet with Post Office to discuss, prior to the consultation, but we are still awaiting this approach.

x. Fit & Proper Test Requirements

59. There have continued to be significant challenges with the Fit & Proper project with considerable oversight and support required by Compliance:

- In February 2019, following further issues delivering the project, there was another change to the project team, with a new Project Manager and Project Management Officer being appointed. This brought better focus and pace to the project.
- Due to early data request errors and delays in writing to agents to collate data, we engaged with HMRC to ask to extend the deadline for the provision of all agent data from June 2019 to September 2019, to enable Post Office to complete the data capture with agents. This was approved by our regulatory supervisor.
- Following extensive follow-up activity and support from the Area Managers in contacting non-compliant agents, branches for which no complete F&P declaration had been received had their ability to transact Bureau de Change and MoneyGram removed on 6th September and 13th September 2019 – 760 branches (445 then 315) were impacted in total. These branches were then given a further 60 days to return their documentation before we de-registered their premises with HMRC.
- In the week commencing 18th November 2019, 85 branch premises were de-registered with HMRC and the steering group approved that any de-registered Agents who subsequently seek to be reinstated, must pay the HMRC registration fee to be re-registered before the transactions are enabled.
- All Commercial Partner data capture and declarations are complete.
- The master data (c. 13k rows of data) continues to be maintained manually on a spreadsheet and there are still a number of gaps in existing processes to ensure that data capture is accurate and optimised.
- When pulling the full agent data against registered premises to send to HMRC for the November monthly submission, it was identified that there were still 625 individuals with missing NINO, DOB, or both. Some of this agent data was held in other systems and could be rectified, however, it was identified that c. 213 agents had never been contacted and therefore had not returned their up to date data and declaration. The data was subsequently rechecked and 193 of these branches had contracts that started in 2019, therefore checks and data capture would have been covered as part of the on-boarding process and the data available in other systems. The remaining 20 branches were made up of

17 sole traders with either partial or full information collected and 3 others where no information had been collected.

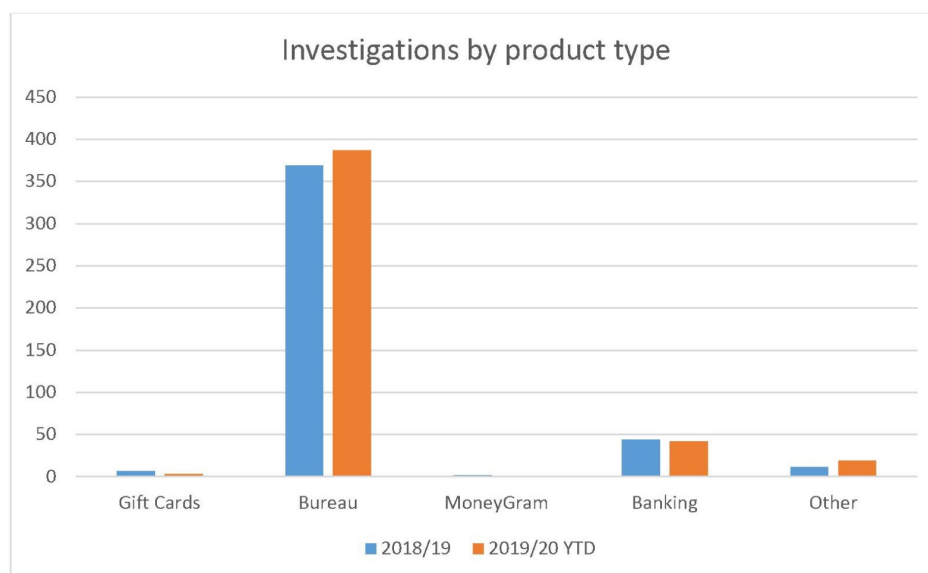
- Letters were sent to these 213 agents on 9th December and it is hoped to close these remaining gaps by January. Our regulatory supervisor has been advised and in the meantime, we will continue to send full agent data lists to HMRC each month to evidence the progress being made. As at 16th December, 181 data anomalies remained, but when preparing data for the December submission it was identified that there were 210 missing NINO and DOB's which appears to be caused by incomplete data being captured by Agent Services. A meeting is planned for January to improve processes.
 - Approval for a Fit and Proper outline solution and high level design has been given by the Enterprise Architecture Group, and in November the Portfolio Review Board (PRB) approved the system in principle and the cost to build it, but have asked the project team for further clarification on the on-going run costs, and a further submission is being made to the PRB 21st January 2020.
 - This new system should resolve a number of the current data integrity issues, but it is likely that there will continue to be issues each month until then.
 - It is anticipated that the new system for generating annual declarations, capturing data and generating the required reporting both for Post Office internal governance and HMRC agent data provision will be built and delivered by 20th April 2020. The first set of annual re-declarations to the first cohort of agents will then be sent end April/early May, with further monthly cohorts scheduled to ensure that all agents are contacted to re-declare annually.
60. Further work will be required throughout 2020 to complete the agent Fit & Proper project and transfer to BAU activity, along with appropriate compliance assurance oversight. This will need to be completed and implemented before the annual registration in June 2020.
61. Following HMRC undertaking 50 agents to test Fit & Proper data in October 2018, we wrote to HMRC in March 2019 setting out our legal view in relation to the F&P requirements for Officers in Charge/Agent Branch Managers (a requirement that would have given rise to significant additional cost). HMRC confirmed that POL does not need to extend F&P requirements to OIC level, however, it has reserved the right to review the position regarding staff undertaking branch management roles as part of any future compliance activity and if it deems, in specific instances, they are within the scope of the relevant guidance, POL will need to submit their details as part of the agent list.

E. Investigations and Incidents

62. There have been 451 investigations up to P8 2019/20 (an average of 56 per month), this is compared to 433 for the whole of 2018/19 (an average of 36 per month). As detailed in the table below, the level of Bureau de Change investigations has already surpassed the number of investigations during 2018/19. This annual increase is expected to continue and accelerate as we implement additional Bureau de Change monitoring reports. Data on operational work

provided to the Travel team will help monitor and determine if further system changes or controls are required in Horizon to reduce manual investigation activity.

63. Banking investigation volumes to P8 are on par with the total seen for the whole of 2017/18, but are also more complex as they have involved multiple branches and bank customers. Each case therefore has taken far longer to work, with access required to several systems to piece together the connections to enable banks and law enforcement to take action.
64. The graph below shows the investigations undertaken in 2018/19 and up to P8 2019/20 and is split out by the high risk products:



65. Bureau de Change (volume and value of branch transactions 2018/2019 & IRRELEVANT and to P8 2019/20 IRRELEVANT & IRRELEVANT).
- Whilst the overall volume and value of transactions is down year on year, to P8 YTD 2019/20 there have been 387 Bureau de Change investigations relating to branch non-conformance, money laundering and confirmed card fraud
 - The introduction of the new AML Credence universe and Business Objects has led to an increase in the identification of potential vulnerable customers purchasing currency. Over a two month period, a customer purchased in excess of £15k in branch and also attempted to place a pre-order transaction for further currency. After intervention by the team, the pre-order was refused and banking protocol initiated. Information provided by law enforcement advised that the customer did not really understand what they were buying the currency for, but believed it was for a timeshare. Another example was a customer who purchased c£44k in just over a month. Open sources research completed and information provided by the branches confirmed that the customer was deaf. This individual was reported as potentially vulnerable to law enforcement and the transactions subsequently stopped.

- As a result of branch non-conformance up to P8 2019/20, 15 branches have been raised to Contract Advisors to take contractual action
- Following the implementation of Microsoft Dynamics 365, the team is now able to record what mitigation has been undertaken for each case. Volumes to P8 2019/20 are as follows:
 - 1044 Branch phone calls
 - 73 text blasts
 - 15 Memoviews
- Compliance has established a relationship with the Risk Director at WHSmith who has requested that any serious concerns/breaches relating to WHSmith branches are escalated directly to him and he will ensure remediation activity is undertaken

66. MoneyGram (volume and value 18/19: send transactions IRRELEVANT receive transactions IRRELEVANT Volume and value to P8 19/20: send transactions IRRELEVANT, receive transactions IRRELEVANT).

- The team continues to meet monthly with the MoneyGram compliance team to review issues, but generally, the number of issues relating to MoneyGram have reduced significantly due to the new controls MoneyGram implemented in 2017.
- During the current year, the network report that vulnerable customers are sending money to Guinea and India. Trends have been identified as fraudsters pose as Microsoft, or request vulnerable customers to send funds in relation to PPI. All reports have been escalated to MoneyGram through our fortnightly SAR update.
- MoneyGram transaction monitoring has identified 75 potential branch non-conformance issues up to P8 2019/20. This has resulted in MoneyGram conducting a review at each branch, either in person or over the phone, to discuss the failings and provide further training. Prior to each review, Financial Crime Compliance has completed a check of each branch to confirm whether any other concerns exist.

67. Banking Framework Services Cash Deposits – Up to P8 2019/20, there have been 42 investigations relating to partner banks, of which, 40 relate to suspicious high volume/value cash deposits. The total amount linked to these cases is IRRELEVANT compared to c. IRRELEVANT across 47 investigations during 2018/19 up to P8.

Over the last year, we have identified a rising number of high value and complex cases relating to business banking deposits which have been referred to Law Enforcement and the relevant banks. As a result, HMRC has presented 3 cases arising from SARs submitted by Post Office totalling IRRELEVANT to the UK's Joint Money Laundering Intelligence Taskforce.

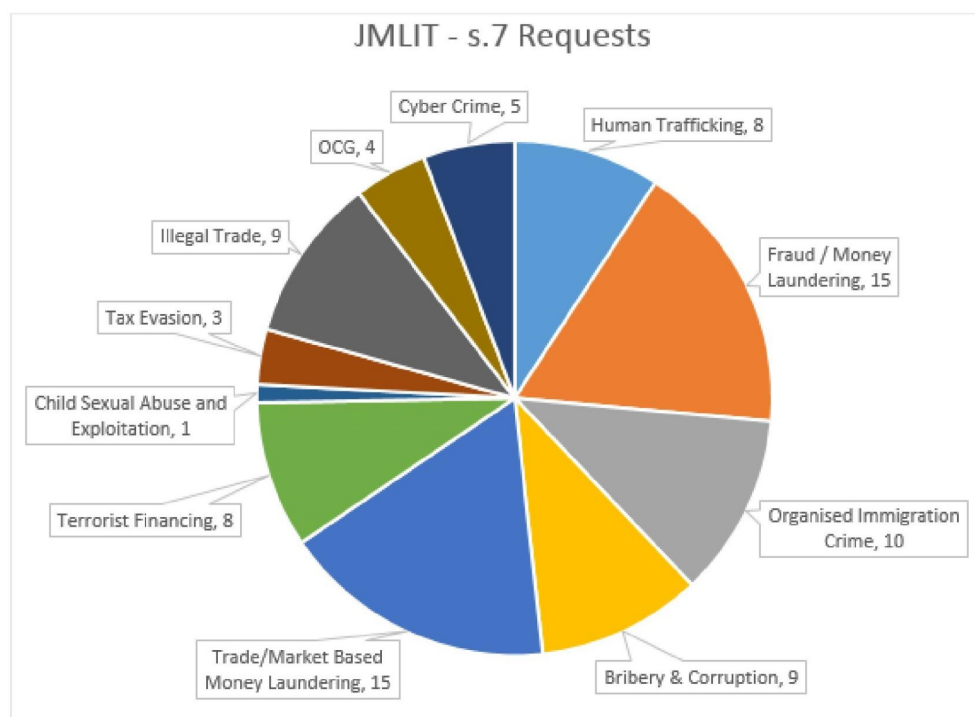
The cases below are examples of high-level investigations the Financial Crime team has managed. These have been identified from intelligence received by Compliance and SARs raised by branches, cash centre staff, area sales managers and third parties:

- A partner bank raised concerns regarding several cards that were being used to deposit high values of cash at two branches located in East London. Following review, high value cash deposits were identified into multiple different bank accounts, totalling c.£15.2m from December 2018 to June 2019. These transactions took place at 52 Post Office branches although the individuals predominantly targeted East London locations. Financial Crime Compliance visited one branch that had been significantly impacted to provide awareness and education. All information has been disclosed to Law Enforcement along with CCTV footage.
 - During June 2019, HMRC advised us about a business customer depositing high values and volumes of cash,. Analysis was completed on deposits made on the 2 cards provided by HMRC which identified a number of potentially linked transactions made into multiple other bank accounts across a number of Post Office branches in the Bradford and Manchester area. The total linked was c.£2.5 m. The main branches were contacted advising them to capture customer details and ID. CCTV was captured and shared with Law Enforcement.
 - Following a SAR raised by the network, high value cash deposits were identified onto multiple banks cards totalling c.£20.9 million from June to November 2019, that appeared to be linked. The individual deposit values ranged from £80 to £16k. These transactions took place at 267 different Post Office branches, with the majority of branches located within the M25 (predominantly East London). We liaised with a number of branches to capture further customer information. CCTV was reviewed which identified 6 potential subjects. All information has been disclosed to Law Enforcement, however, activity remains ongoing.
 - Supply Chain raised concerns that a branch had recently increased its cash collections. It was identified that high value cash deposits were being processed onto twelve cards issued by multiple banks. A total of c.£10.5m was deposited over 7 months at 13 branches. Details were shared with the banks who then conducted a review of the accounts and details of our investigation were shared with HMRC. The main branch targeted by this group was visited by Financial Crime Compliance and advised that future transactions must be declined unless the customers were able to provide personal ID to confirm their identity.
68. One4All Gift Cards (GVS) – A report containing the total remuneration paid for gift card sales broken down by branch over a 12-month rolling period is received and reviewed by the Financial Crime team on a monthly basis. One branch was identified due to a spike in gift card sales during July 2019 (August 2018 to June 2019 – the branch average monthly sales value was £67, but in July 2019, £44k of gift cards sold). Following a conversation with the branch, it was identified that all cards were for a single individual who had said they recently sold their business and were purchasing the cards as a gift for all company employees. On referral to GVS, they advised that the gift cards remained inactive with their full balances remaining. Following further conversations with the branch, the agent advised that in order to facilitate the large order, the customer transferred the funds to the agents own account via bank transfer and he purchased the gift cards using his own debit card. The agent explained that he did contact NBSC who did not advise that this was unacceptable. This information has been confirmed with NBSC and the agent has been made aware that this is a breach of the sales process and must

not be repeated. This was also escalated to the Head of NBSC to implement further training to call handlers

69. Card Fraud over Post Office counters – Between 1st January 2019 to 15th November 2019 there were 2122 fraudulent transactions processed to the value of £228,519.64; with the majority of transactions over £100 relating to Gift Card purchases. Card fraud has declined compared to last year, where there were 3,009 transactions totalling £425,635.35. YTD there have been no Card Scheme breaches.
70. The volume of JMLIT s.7² requests received and worked by Financial Crime Compliance to P8 2019/20 has remained consistent with last year, however, the volume of subjects (individuals) requiring checks has doubled:
- s.7's requests received - 87 (95 during previous year up to P8)
 - Number of searchable subjects included in the requests – 1060 (566 during previous year up to P8)
 - Number of subjects identified in Post Office data – 36 (41 during previous year up to P8)
 - Following the recent terror incident at London Bridge on 29/11/2019, Financial Crime Compliance remained on 24/7 call to support urgent requests from the National Terrorist Financial Investigation Unit. No links to the Post Office were identified from checks completed.
 - The chart below shows the underlying issues relating to each request for information received from JMLIT:

² Under section 7 of the Crime and Courts Act 2013, the NCA is empowered to request information for the purposes of exercising any NCA function, responses to these data requests are a key activity for JMLIT members.



F. External Threats/Landscape

i. Business areas

71. There have been no significant changes to the Post Office regulatory landscape during 2019 as a result of changes in the Post Office.

ii. Fifth Anti Money Laundering Directive

72. Post Office submitted a response on 10th June 2019 to the HMT consultation on the transposition of 5th Money Laundering Directive (5MLD) into UK law. The following concerns/clarification requests were raised:
- the inclusion in the UK Politically Exposed Persons (PEPs) definition of "Board members of for-profit enterprises in which the state has an ownership of 50% of more, or where reasonably available information points to the state having control over the activities of the enterprise", which would bring Post Office Board members into scope for PEP due diligence in their personal financial dealings.
 - the extension of the regulatory definition of 'officer' to 'managers', and that this should be 'senior managers' to align with the FCAs Senior Manager Regime
 - whether customer due diligence is required as a distributor of third party manufacturing pre-paid cards

- we are also asked that the Government recognised the GOV.UK Verify scheme under the provisions for electronic customer identification
73. Due to delays in Brexit and the General Election, no draft legislation for the 5MLD has yet been published. With an implementation deadline of 10th January 2020, it is suspected that the legislation will either be published as a final version on or around 10th January or it will be delayed. The legislation will need to be reviewed to check for Post Office impacts, and the outcome of this review will be reported to the subsequent Post Office RCC and ARC.
74. In readiness for the reduced limit for anonymous prepaid cards under 5MLD, GVS are reducing the maximum load limit on One4All Gift cards from £400 to £120 from the 10th January 2020.

iii. Supranational Risk Assessment

75. In July 2019 a Supranational Risk Assessment of money laundering and terrorist financing activities affecting the internal market and relating to cross-border activities was conducted by the Commission to the European Parliament and The Council. The report highlights that cash remains the number one choice for criminals to money launder, as well as cash like assets. It also highlighted vulnerabilities in all sectors such as criminals obtaining employment within organisations, new technologies assisting criminals to create better counterfeit documentation, insufficient information sharing between public and private sectors, insufficient compliance resource and awareness, and risks emerging from FinTech products.

iv. Office of Financial Sanctions Implementation (OFSI) Penalty

76. In June 2019, OFSI published a penalty noticed imposed on Travelex (UK) Ltd for a bureau de change transaction. A penalty of £10,000 was issued due to a single transaction of £204 breaching the EU Egypt financial sanctions regime. This was in addition to a £5,000 penalty for Raphaels Bank in relation to the same transaction issued in January 2019. These fines demonstrate OFSI's readiness to exercise its civil monetary penalties wherever it is deemed appropriate, and not just on large cases/values.
77. Post Office currently undertakes Sanction screening for all on-demand and pre-order Bureau de Change transactions over £2,000 as part of an electronic Know Your Customer (eKYC) check. We also undertake ad-hoc checks as part of investigations. To date Post Office has never had a Sanctions match, and the risk is deemed low.

v. HMRC compliance and registration penalties

78. In 2019, HMRC announced a record fine of £7.8m against Touma Foreign Exchange Ltd, for Money Laundering Regulations breaches between June 2017 and September 2018. This included failures within its Fit & Proper (F&P) tests, risk assessments, policies, controls and staff training. This highlights the pro-active approach HMRC are taking to tackle money laundering and regulatory non-compliance, and the potential public penalties possibly imposed. This approach indicates that should Post Office fail to comply with money laundering regulations, we would incur a penalty much greater than our previous fines under the 2007

MLRs which totalled c.£1.1m, additionally under the 2017 MLR's these fines are now made public, prior to any appeal process.

v. Other regulatory developments:

79. The Foreign & Commonwealth Office published guidance in July 2019 explaining how the UK would implement sanctions if the UK leaves the EU without a deal. The UK would implement UN sanctions in UK Domestic law after the UK leaves the EU, as required by international law. If there was no deal, then the UK would carry over all EU sanctions at the time of departure. The government will implement sanctions regimes through new legislation, in the form of regulations, made under the Sanctions and Anti-Money Laundering Act 2018 (the Sanctions Act). Any sanctions that the UK did not address will continue as retained law under the EU withdrawal Act 2018, ensuring there are no gaps. UK will publish the names of sanctioned persons or organisations, and regulations would be published as normal alongside guidance
80. The Financial Action Task Force (FATF) has shared draft guidance on digital identity (digital ID) for public consultation. This guidance is to clarify how digital ID systems can be used for customer due diligence (CDD). The draft guidance intends to help governments, financial institutions and other relevant entities apply a risk-based approach to the use of digital ID for CDD. Guidance is intended to assist governments, regulated entities and other relevant stakeholders determine how digital ID systems can be used to conduct certain elements of customer due diligence (CDD) under FATF Recommendation 10.

G. Conclusions and Recommendations

81. The regulatory environment continues to pose a challenge, with increased regulatory and legislative focus on money laundering and terrorist financing. Following the 2018 FATF UK Mutual Evaluation review, there is evidence of increasing focus by regulators, and readiness to exercise monetary penalties, as evidenced by OFSI and the FCA. We have also seen a more pro-active approach to supervision by HMRC (funded by the significant increase in registration fees from 1st May 2019) and an increase in the volume and scale of penalties issued by them. This indicates that should HMRC identify that Post Office has failed to comply with money laundering regulations, penalties will be more egregious than historically, as well as being made public. It is therefore important that Post Office's commitment to comply with all aspects of regulatory requirements remains high on the agenda.
82. The Supranational Risk Assessment issued on 2019 highlights that cash remains the number one choice for criminals to money launder, and this has been borne out by the increase in suspicious activity that has been identified through the year relating to Banking Framework cash deposits over Post Office counters
83. Political uncertainty has delayed publication of the draft UK legislation relating to the 5MLD, but it is still expected that this will be enacted by 10th January 2020, and therefore the final content and Post Office impacts are unlikely to be known and assessed until after publication, including the likely impacts of Politically Exposed Person status for Post Office executives.

84. The establishment of the NECC in October 2018, has seen an increased focus in activity, and this is borne out by the increased workloads we have seen responding to subject requests, which have doubled year on year. A number of the cases under review relate to cash-based criminal activity with a predominance in human trafficking, organised immigration crime, modern slavery and sexual exploitation.
85. The HMRC supervisor who has overseen Post Office regulated activity since 2015 is retiring in June 2020, and therefore Post Office will have a new supervisor during the early part of 2020, which may bring changes to HMRC regulatory oversight and activity. We are also aware that HMRC are considering a further review of their registration fee structure, although as yet, there has been no guidance on this.
86. Further work has been undertaken to resolve data issues with the Bureau de Change monitoring solution and assessment and oversight of the product continues to mature. The increased volumes of investigations and SARs evidences the improvement in controls since the HMRC audit in 2016 and subsequent penalties. The new premises registration reporting tool was delivered by DCoE in 2019 and has improved the accuracy of registration data, however, some further work is required to generate the HMRC reports in the correct format and remove manual manipulation. Customer Due Diligence, PEPS and Sanctions checks for Bureau de Change are currently assessed to be adequate.
87. The agent Fit & Proper data requirements have continued to be a significant challenge for Post Office, and data gaps and challenges remain in providing accurate monthly reporting to HMRC due to the disparate systems that store the information. Significant effort was required to meet the extended deadline of September to complete the data gaps, although ultimately only 85 premises were deregistered, albeit further data discrepancies were then identified. Data issues are likely to continue until the new data system is designed, built and delivered in 2020. Additionally, due to the high number of structural changes within Post Office over the last 12 months, it has proven difficult to keep the direct employee Fit & Proper tests up to date with HMRC, and the business is giving insufficient review of regulatory oversight responsibilities when changing reporting lines and/or roles, which must be addressed moving forward.
88. Following increasing workloads over the previous two years, two additional financial crime roles were created and recruited into Financial Crime Compliance during 2019. This has ensured that enhancements could be made to Bureau de Change transaction monitoring and investigations, and the back log of risk assessment work has been brought up to date. This has also meant that more focus can be given to industry and regulatory horizon scanning to ensure that Post Office is adequately protected. The team have also absorbed the continued increase in investigations (up 40% compared to 2018) and SARs (up 35% compared to 2018), although if this trend continues, this will not be sustainable, and there is limited, if any, automation that can be introduced to cover these tasks.
89. Products and services provided by Post Office are broadly in line with the risk appetites set by the Board and, with the exception of the Banking Framework services, there has been an improvement in residual risk over the last 12 months. The Bureau de Change residual risk continues to improve as increased controls

and improvements to transaction monitoring are implemented. Risk Assessments for Post Office Insurance have fallen behind due to product managers failing to complete Product Information Packs/respond to queries in a timely manner and this has been highlighted to the POI ARC. First line compliance with Post Office policies is of concern and further work will be undertaken in 2020 to improve first line management awareness of the policy minimum control requirements that are their responsibility.

90. Work has commenced to undertake assurance activity in respect of Payzone products and services. There is currently a lack of documented policies and procedures to support this area of the business, but it is hoped that this activity this will be concluded by the 2019/20 financial year end.
91. There have been a number of high value and high profile investigation cases relating to money laundered through Post Office counters via accounts held by banks operating within the Banking Framework. As a result there has been significant interest and focus by various law enforcement organisations culminating in the establishment of Project Admiralty by the NECC with key stakeholders to address the risks and issues. Up to P8 2019/20, Financial Crime Compliance have investigated and raised SARs relating to c. £92m of cash deposits. Product Management and Compliance must ensure that adequate focus and support is given to industry, NECC and Post Office initiatives to address the migration of cash placement risks to Post Office as banks close, including following through on the actions recommended in the Banking Framework risk assessment.
92. Whilst overall, there has been a significant improvement to mandatory training compliance in the Network, brought about by the roll out of SmartID and training controls, training and awareness remains a key control for AML/CTF and challenges remain:
 - Whilst all Horizon users now complete the training and test, it is evident from branch visits by Financial Crime Compliance that the key messages are not landing, and branches are sometimes failing to question transactions or report suspicions, either because they lack confidence, or because they do not understand how to apply the training. With the current method of delivery of training via Horizon, there is limited scope to improve the content, and Financial Crime Compliance will continue to work with the Area Management team and the NFSP to identify different ways to deliver key messages.
 - We are looking to design and deliver animations as part of the annual AML/CTF training in May to help land key messages, but as these cannot be incorporated into Horizon, alternative access will be needed for the Network
 - There are still challenges with back office staff completing training within the required deadlines, and this continues to be monitored and chased by Financial Crime Compliance.



Post Office Limited Audit, Risk and Compliance Committee Report

Title:	Business Continuity and Resilience Update
Meeting Date:	28 th January 2020
Author:	Tim Armit, Business Continuity Manager
Sponsor:	Jeff Smyth, Digital Technology Director, CIO FST & Identity

Input Sought

Action Required: Discussion	Noting
Previous Governance Oversight:	Risk and Compliance Committee, January 2020

Executive Summary

Context:	<p>Business continuity solutions and levels of resilience continue to increase across all operational areas of Post Office.</p> <p>Solutions have all been tested and proven to meet business requirements.</p> <p>Response, escalation and incident management teams and plans are in place and fully functional.</p> <p>People, facilities, IT and supply chain are the main areas of risk and each has been considered and mitigated where possible.</p> <p>IT issues have increased over December but with minimal impact on customers and income.</p> <p>GLO and RMG industrial action have both led to increased levels of readiness.</p> <p>Key Risks:</p> <p>The business response to a complete Horizon failure The sudden loss of a Retail Partner The loss of the Telco datacentre</p>
-----------------	---



Questions asked & addressed

1. Do current levels of resilience and continuity plans in place meet Post Office requirements?
2. Are there key business continuity risks the Post Office is exposed to?

Report

3. Do current levels of resilience and continuity plans in place meet Post Office requirements?

Yes, the current approach to resilience and continuity ensure that Post Office can respond to major incidents in a timely and controlled manner.

Physical relocation solutions for Chesterfield, Bristol, Bolton and London are in place with Sungard and these have all been tested and proven to work.

Incident response and escalation methods are in place for all levels of incident. A new sub team to respond to branch incidents has been stood up and proven which links into the Business Protection team (BPT). The IT incident response team and its links to the BPT are proven and known by all involved.

A new strategy and tool was deployed in December. This is the Post Office on Wheels which enables an entire branch with all services and technology to be delivered with 24 hours to any location. It is simply plugged in, connected to the internet and made live. This has been deployed live in December. The concept was first considered in September 2019 and implemented in December 2019. The Post Office now has a solution, which for the first time in its history, can mitigate the sudden loss of a branch (due to fire, flood etc) or a key retail partner.

Grapevine, a third party security supplier to Post Office, has in place a system to send texts and other forms of communication to every branch, office and members of staff if other communications systems are not operational or it is out of working hours. This has been proven to work and has been used in December during the Verizon datacentre failure incident.

The incidents across December which impacted administration offices, call centres, SSK's, the ability for customers to use card payments, ATM's and Moneygram and access to the vault at Hemel were all unrelated and had almost no impact on customers or income. The Verizon data centre which stopped all operations in every administrative office did not affect branches or customers (there were no customer complaints or comments on levels of service). Whilst there was some frustration in card payments failing, many worked on the second attempt and or customers could withdraw cash to pay, this again led to no noticeable service impact or customer complaints. This pattern continued across the other incidents.

The Resilience manager is working with IT on the root cause analysis of the plethora of incidents; as the link between increased volumes of business and incidents in December correspondingly increases the level of risk to service.

The planning for a response to the GLO ruling and to the threat of RMG industrial action was inclusive of contingency responses. The RMG planning exposed a number of risks to Post Office operations which will require further consideration, particularly to the amount of Post Offices RMG planned to collect from and the number of daily collections, both of which had significantly reduced from the planning levels in 2017. The industrial action has now been called off.



4. Are there key continuity risks the Post Office is exposed to?

Yes, there is no coordinated strategy for the large scale failure of the Horizon system; this risk was identified in late 2018 and work was completed across all products and business areas. Manual operations are not possible for many products and due to increased Regulatory changes some strategies can no longer be considered in the Banking area. There are no standing instructions in branches as to what is expected of them and currently if Horizon fails most branches would close and remain close until it is restored. The four key pillars of operations:

- POCA – emergency cash payments can be made to customers but this would be at the Post Office's risk and would be noted on paper for later reconciliation.
- Payment – Customers would be directed to other local payment systems.
- Banking – Cheques could be accepted but not processed until the system is restored, customers would be informed of this and can choose not to use Post Office.
- Mails – ongoing discussion with RMG as to what scale of offer could be made. Stamps can be sold for cash but no special services could be offered currently.

These operations are then measured against branch accessibility to determine priority branches.

Any ongoing operation would be paper based and the Post Office would be at risk on every transaction and would have to ensure Post Masters understood where the risk lay, with Post Office not them. This increases the risk of mistakes and fraud.

Ongoing work with product teams and IT on alternative solutions continues. The key is to ensure the systems are fully resilient in design with automatic fail over and uninterrupted service.

There is a key risk of the sudden loss of a Retail Partner. Work has been undertaken to identify how a response would be managed and what strategies could be used to mitigate such a loss. In the worst case scenario over 600 branches may close their doors to customers. Whilst the plans utilise every effort to re-open these branches with differing strategies it is agreed that approximately 80 branches would need to be opened within 2 days to serve POCA and vulnerable customers, where no alternative branch or service exists. To mitigate this the Post Office on Wheels has been developed and there is a commitment to build 100 of these devices by April 2020. These solutions will enable a branch to be opened within 48 hours in local church halls, or town halls etc and for service to vulnerable customer to be maintained. All other branches are within an acceptable distance of another branch to provide service.

The datacentre supporting back office processes of the Telecommunication business within Post Office has no planned recovery capability. The contract contains no disaster recovery provision meaning if the datacentre is lost Fujitsu post event would attempt to source replacement hardware to build an environment in an unspecified time with no known costs for doing this. A new supplier will be brought in for this contract but this could be over a year away.

Financial Impact

5. None directly but will need additional budget to mediate risks.

Risk Assessment, Mitigations & Legal Implications

6. None Directly



Stakeholder Implications

7. Resilience and continuity uniquely covers every aspect of infrastructure, operations and leadership as well as external supply chain, as such it liaises and supports stakeholders in all areas.

Other Options Considered

8. Not Applicable

Next Steps & Timelines

9. Focus on Horizon resilience levels and continue to develop alternative working practices.
10. Support IT in reviewing root cause analysis and ensuring operational mitigations continue to meet business needs.
11. Escalate the Post Office on wheels solution.



Appendix 1

None included.



Post Office Limited Audit, Risk & Compliance Committee Report

Title:	Audit, Risk & Compliance Committee Report
Meeting Date:	28 January 2020
Author:	Mark Baldock: Head of Risk Jonathan Hill: Director, Compliance Johann Appel: Head of Internal Audit
Sponsor:	Al Cameron: Chief Financial Officer Ben Foat: General Counsel

Input Sought

Action Required:	Noting
Previous Governance Oversight:	

Executive Summary

Context:	The paper provides an update on key and emerging risks, compliance matters and an update on the latest internal audit position.
Questions asked and addressed:	<ol style="list-style-type: none"> The committee is asked to: <ul style="list-style-type: none"> <u>note</u> the current key enterprise risks <u>note</u> Central Risk are undertaking a review of all active/emerging enterprise (and key operational) risks. This will be presented to GE in February with a re-baselined position reflected in RCC/ARC paper in March 2020. <u>note</u> the key intermediate/business risks <u>note</u> the emerging enterprise risk around End of Life components <u>note</u> the latest position on Brexit <u>note</u> the latest position on the implementation of the Post Office's Governance, Risk & Compliance tool (Archer) <u>note</u> the status of the Change Portfolio and its current top portfolio risks and key delivery challenges <u>note</u> the Compliance update with particular focus on the conclusion of Ofcom's Text Relay investigation, PSD2 & Telecoms, the current approach to meeting the new Cookies requirements and the progress made on Contract Remediation <u>note</u> the progress being made with delivery of the Internal Audit programme and completion of audit actions



Risk

What are the key enterprise risks and what is the business doing to address these?

- 1 The Post Office currently have 13 active enterprise risks. A complete list is provided at Appendix 1. Central Risk are now undertaking a review (and potential refresh of all active/emerging enterprise (and key operational) risks which will be presented to GE for discussion and approval in February. This re-baselined position will be reflected in the RCC/ARC paper in March 2020. In the meantime based on their current RAG scores, the key enterprise risks facing the business are Payment Card Industry Security Standards (PCIDSS) (4:4), Retail proposition (5:3), Brexit (4:3) and Group Litigation (5:3).

What are the key Intermediate (Business) Risks and what is the business doing to address these?

Business Continuity

- 2 During the last quarter of 2019, there were a number of incidents that impacted the business operations, namely outages around SSKs, VPN and BoI transactions. Although these incidents were remediated, they were outside of service standards. Root cause analysis is underway to ensure future resilience. Work is planned to review the level of business reliance and the robustness of contingency plans in place. An associated business risk will be articulated as needed.

Payzone Risk Management Framework/Workplan

- 3 Payzone continue to work towards the development of a wider Risk Management Framework. The management team have reviewed the risk register and agreed target risk scores with mitigation plans and target dates in place. A process flow chart detailing the correct risk management processes has been generated and submitted to the POL Central Risk team for further review. A risk workplan has been created to monitor and update the management team on progress on key risks and activities, including progress to address significant risks and return to acceptable levels. We consider the following risk should be noted by RCC.

Risk	Mitigation Plan	Current Score using Payzone I/L	Current Score using POL I/L
The urgency in deploying a permanent fix for an existing terminal pairing issue (between devices E200 and T103) affecting agent and customer transactions may increase with on boarding of high profile clients. If agents are unable to carry out the transactions there will be significant impact to customers, particularly vulnerable.	Following the on-boarding of a dedicated contractor, significant progress has been made on defining the issues (mainly around Terminal pairing and WiFi connection). A number of additional fixes are planned for deployment, however, currently on hold to ensure stability of service whilst in 5 day consecutive operation test and in readiness for 1st Jan exclusive service. Unlikely to release before mid-January. Plan to be developed to communicate to retailers on resolution process for pairing issue in order to reduce the impact to the helpdesk.	20 (4:5)	9(3:3)

11

What are the emerging risks faced in the short and medium term and what is being done to address these?

- 4 An emerging IT risk (4:3) has been identified around a potential number of hardware and software components managed by our various 3rd party suppliers which may be 'end of life'. IT are assessing these components to determine their actual status and will upload the baselined position into Service Now to allow for proactive configuration management.



- 5 We will be undertaking a deep-dive on this risk (along with confirming the current underlying IT business/intermediate risks) as part of an IT risk workshop in early February 2020. The outputs of this work will be a baselined suite of IT risks which will be uploaded into Archer as part of the wider deployment of the GRC tool.

What is the latest position on Brexit?

- 6 The Conservative party secured an 80 seat parliamentary majority as a result of the December 2019 General Election. At this point the Withdrawal (Agreement) Bill (WAB) is expected to complete its UK and EU Parliamentary ratification in January 2020 allowing the UK to leave the EU on 31 January 2020.
- 7 UK Whitehall Departments are now turning their attention to preparing for the UK-EU Free-Trade Agreement (FTA) negotiations. The objectives, scope and sequencing for these negotiations still need to be finalised on both the UK and EU sides. The nature of the FTA negotiations (and their impact on Post Office) will be significantly influenced by the timeframe.
- 8 We advised RCC/ARC in November 2019 that, as drafted, the WAB regards Northern Ireland as part of the EU Customs Union. If unamended during the FTA negotiations this may require RMG/Post Office to adjust their current GB and NI mail process to allow for the completion of EU custom declaration forms for post being sent from the UK to NI. There may be need for changes to Horizon to cater for multiple VAT rates (as NI may need to align with the Eire, rather than UK).

What is the latest position on the implementation of the Post Office's Governance, Risk & Compliance tool (Archer)?

- 9 The Central Risk team have embarked on implementing Archer (an industry standard GRC tool) to enhance the efficiency of our risk management. We have successfully designed, built and achieved a technical go-live for the Archer Phase 1 solution allowing exclusive deployment to the Central Risk team. Immediate next steps are for us to quality assure and then upload all Post Office enterprise risks into Archer. This will be followed by cleansing and uploading all Post Office business and local level risks to the system. We are currently working on a comprehensive Archer deployment plan with the intention of commencing from February 2020 with an aspiration to complete by June 2020. In parallel, by end of January 2020, we will have put in place a GRC corporate governance body to oversee the Post Office's GRC Strategy and supporting framework as well as the design and delivery of Post Office wide GRC processes.

11

What is the status of the Change Portfolio, including top risks and key delivery challenges?

- 10 The overall status of the portfolio remains Amber. The temporary 'pause' on new funding requests has now ceased. Prioritisation and increased scrutiny of spend and benefits has increased confidence we will remain within 2019-20 budget. Progress continues across gold/platinum projects with 1 project closed and 2 projects completing successful implementations in P8. The portfolio has seen a slight increase in the number of gold and platinum projects reporting an overall RED rating for the Risk RAGs. This has resulted in the portfolio risk RAG status being upgraded to Amber which, in turn, has contributed to the portfolio status remaining at Amber.



- 11 There has been a decrease in the number of gold and platinum projects reporting an overall Red RAG status from 7 to 5. 3 projects remain RED from November (PCI; IDS Digital Identity; Digitising Mails). The 6 Red RAG projects are:
 - PCI Compliance (Cost, Risk and Overall Red RAG): Ingenico costs are £1.5m in excess of what was expected as a result of changes made to the technical solution. Final commercial agreements with Fujitsu/Ingenico, Computacenter and Vocalink under review by vendor management, legal and delivery teams.
 - IDS Digital Identity (Cost, Benefits, Delivery, Risk and Overall Red RAG): The primary supplier is not able to deliver the requirements. Discussions underway on options for a way forward. Investigations underway to find another supplier.
 - Digitising Mails (Cost, Benefits, Delivery, Risk and Overall Red RAG): Reporting Red as spend is on hold while business evaluates various delivery options.
 - POCa replacement bid (Risk Red RAG): Risk of reputational damage through the choice of DWP's replacement solution (a paper voucher service). Post Office is not supporting this solution as vulnerable customers could be left without easy access to legacy POCa balances as the voucher service will not allow balances to be transferred.
 - Legal Entity Optimisation (Delivery & Overall Red RAG): LEO scope is focused on putting in place appropriate governance. Underlying work including Route to Dividend, Articles of Association (AoA) and Framework Documentation agreed. Formal PO, POI Board and Payzone Boards will take place between January and March 2020. A Change Request will be progressed to reflect new timescales bringing project back to green.
 - Parcel shop (Cost & Overall Red RAG): Red due to funding and scope not being fully aligned as the project made changes out of governance. A change request for retrospective approval is progressing.
- 12 Appendix 3 provides a summary of the current key 'Platinum and Gold' change programmes and their current reporting status.

Compliance

Telecoms

Text Relay

- 13 Ofcom has sent us an "S96 Notice" of our breach of the General Conditions in relation to Text Relay. This is a formal step in the investigation, which was expected. The notice is based on Ofcom's Statement of Facts sent earlier in December. Ofcom had the potential to fine Post Office up to £11.4M but this was unlikely. More probably the fine was expected to be between £200K and £1.5M. Following representations from Post Office Telecoms and Compliance Ofcom has opted to penalise us £175K (£250K including a further 30% discount for early settlement).
- 14 Early settlement was only possible if we accepted liability for the text relay failing, accepted the fine and waived rights to any further defence by 19th December, which had to be made by a statutory director. We had no dispute with Ofcom's Statement of Facts and as a result agreed to Ofcom's decision in a letter from Alisdair Cameron, dated 18th December 2019.
- 15 We have requested that all individual names (in Post Office and Fujitsu) names are redacted along with commercial sensitive data, in line with Ofcom's request on confidentiality.
- 16 Ofcom has now published a summary of its findings and the fine on its website. We have had limited media enquiries to date, which Group Communications are managing.



PSD2 & Telecoms (there will be a verbal update at the Committee meeting)

- 17 As discussed at the July 2018 RCC and ARC, the Payment Services Directive 2 (PSD2) came into force for electronic communications firms in January 2018. Telecoms firms had the option to apply to the FCA for a full payment institution licence or opt for an exemption, agreeing not to charge customers over a certain amount for premium rate services. The latter requires an annual independent audit to confirm compliance.
- 18 Legal guidance on PSD2 relevance to Post Office Telecoms was varied but it was confirmed in February 2019 that Post Office Telecoms does need to meet the regulations and the Telecoms team was advised it needed to implement the changes. It has been reviewing options and working with its partners/suppliers to make the necessary operational changes and register an exemption with the FCA.
- 19 On 14th January 2020 we notified the FCA that we will be applying for an exemption and that we are developing remedial actions to reimburse impacted customers and implement a technical billing solution. The FCA may seek further information from us on our remedial plans and also seek to impose a penalty given the PSD2 regulations required an ECE to be in place from January 2018. However, to date, the FCA has not fined any firm on this matter. We believe that there are a number of firms in the industry that are not applying the regulations, hence the FCA's 23rd December 2019 reminder to the industry of the PSD2 obligations.

Data Protection

Post Office use of Cookies on Internet and Apps

- 20 Recent updated guidance from the Information Commissioners Office has clarified the management of cookies. There has also been relevant case law handed down (Planet49 fined approx. £4M for non-compliance) from the Court of Justice of the European Union.
- 21 Post Office's current position is non-compliant with both the guidance and case law. However, it is similar to the approach being adopted by many in the UK. MIT, UCL and Aarhus University have conducted a joint study into the use of cookies, analysing cookie management platforms used by the UK's top 10,000 websites. Their research has found that only 11.8% of the sites have met the minimal regulatory requirements and, of those that do, under 13% made the "reject all" option accessible through the same number or fewer clicks as the "accept all" option¹.
- 22 The Digital, Legal and Data Protection teams are working on solutions to be taken forward for consideration and approval. These will be presented to the GE in January. It should be noted that all solutions could have a significant impact on our data analytics and marketing activities (potential impact could be as high as a loss of 93% of permissions granted).

Contract Remediation (GDPR)

- 23 Work has commenced on the Contracts Remediation programme as outlined previously. The outstanding contracts have been considered, categorised and prioritised against streamlined criteria with focus on risk to personal data.
- 24 Considerable progress has been made, with nearly all contracts being sent "deemed consent" letters either as a means of closing down contracts where the counterparty has not responded to date, to close non-material agreements where no contact had so far been made or to initiate contact with Material/High Risk contracts that need action. The

¹ Source: BBC News article 15.01.2020



last category of contracts will be followed up directly by the team to resolve, alongside those already in remediation.

- 25 The programme is scheduled to conclude by end June 2020.

Payzone BPUK:

- 26 An initial review of Payzone Bill Payment UK against the provisions of GDPR was completed in early December 2019.
- 27 The report shows that there is considerable work that needs to be completed in the New Year. However, from a data protection perspective the biggest risk relates to the personal data held on their employees and not that of customers.
- 28 The DP team will be working with PZBP UK to introduce the necessary changes and updates in Q4.

Freedom of Information

- 29 Since the ruling was handed down in the GLO case we have received 2 Freedom of Information requests linked to the case, one from a known individual and linked to the trial.
- 30 Prior to any information being disclosed as part of our statutory obligations responses are being verified by Legal, Retail and Comms to ensure they are consistent with what may have been released previously.

Financial Crime

Anti-Bribery and Corruption ("ABC") update

- 31 Following completion of the Anti-Corruption Government Supplier questionnaire, there was a recommendation that Post Office should publicly disclose its charitable contributions, sponsorships and political contributions. We are currently working with the Corporate Responsibility team to identify the best channels to communicate this, although we state in our Annual Report (Directors Report section) that the business does not make political contributions.
- 32 In the lead up to Christmas, communications have been sent out to remind colleagues that all gifts and hospitality must be reported via the online tool.
- 33 Gifts & Hospitality reporting and approval levels are currently being reviewed and benchmarked against industry best practice, and the new reporting and approval portal is currently being tested and finalised, with rollout anticipated in Q4.

Whistleblowing Update

- 34 Due to the number of reports received recently from Agent assistants, we are currently working with the Communications team to identify ways to raise awareness of the importance of whistleblowing to our agents and ensure they understand that whistleblowers are protected by law to stop them being treated unfairly or losing their job because they "blew the whistle".
- 35 Expolink Europe Ltd currently provide our Whistleblowing Speak Up service, however, the contract has expired. During the contract renewal discussions, Expolink were acquired by Navex Global Ltd, and they advised that they are not prepared to sign a novation in relation to Expolink, but would migrate Post Office onto a contract with Navex Global. It has been agreed internally, supported by Legal, and with the supplier to proceed with the new contract, which would see Post Office migrated onto a new platform with additional services. This is expected to be completed by financial year end.



Fit & Proper update

36 See separate MLRO report

Regulatory updates

37 See separate MLRO report

External Threats

38 See separate MLRO report

Supply Chain Compliance

39 One site audit was completed in November, with 5 Improvement Needs identified, and an audit score of 11, which is on par with the audit last year and no repeat findings. No site audits have been undertaken in December.

Financial Services

Mystery Shops

- 40 Following the finalisation of the Purpose, Strategy & Growth work, the Product Teams and Network will review the approach to FS sales in the network, addressing the on-going compliance conformance challenges.
- 41 Key issues identified continue to relate to Travel Insurance (non-disclosure of medical information and product information) and Life Insurance (not introducing the whole range). There have been no BoI savings red shops in the last 2 months.
- 42 A thematic review was completed for Travel Insurance in November to better understand the issues using targeted scenarios. The results show the same issues as in previous shops. Changes have been made to simplify the questions used in Q4 to further understand the results and confirmation of the current mystery shop results.
- 43 Project Phoenix is due to launch mid-March 2020 with branches offering the same levels of cover as available online. This should enable branches to complete more sales and offer better customer outcomes. Post Office Conduct Compliance is working with POI product and Compliance and Post Office L&D function to create training materials. Face to face meetings with the Network Field teams are planned for Q4 to help understanding of the changes, including the sale process.

Video Mystery shop for Customer Relationship Managers

- 44 Results for Life Insurance in October and November continued to show the same issues with 6 out of 35 videos graded red. POI is currently undertaking a review of its sales strategy through the branch network. One of the key changes will be the removal of the Easy Life product from the CRM Tablets from 31st January. No reds were reported for Savings video mystery shops in October or November.

Capital One Credit Cards

- 45 Capital One appears very risk averse for a small planned pilot on network lead generation. We have prepared and shared a customer detriment risk assessment and are working with its compliance team to help it understand how the Network works and how this activity is managed.



Policy Update

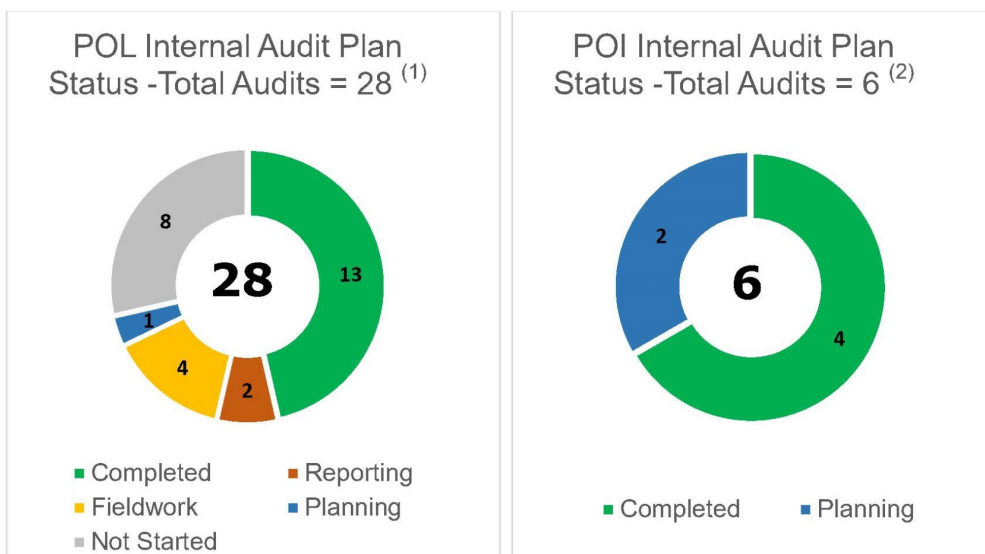
- 46 There is only one new combined policy being updated in this cycle combining Information Security, Cyber and Access.
- 47 Further to the challenge issued at the last ARC it has been confirmed that Group Policies do apply to POI unless for a specific regulatory reason POI is required to have separate policies. Even then it should follow the direction and group approach as far as possible. e.g., POI would be expected by the FCA to have its own separate risk policy and risk appetite, but this should be managed within group risk expectations and processes.
- 48 It has been agreed the Group Change Policy (approved at the last ARC) does apply group wide and POI is not excluded from the policy, a small update reflecting this will be put in place.
- 49 During 2019 with the temporary benefit of a Policy Manager we begun the work of rationalising the policy set from 125 policies to around 30 and ensuring that out of date policies were reviewed and approved. The current focus with the resources available is to work with policy owners in getting them to ensure policies are reviewed on time in the appropriate template.



Internal Audit

Progress against plan

1. Delivery of the 2019/20 programme is making good progress, having finalised four audits since the November ARC meeting (3 POL and 1 POI).
2. Current delivery status is as follows:



⁽¹⁾POL ARC approved baseline plan for 2019/20 (18 core internal control reviews & 10 change assurance reviews). Details of the audit plan status are included in the reading room (Appendix 4).

⁽²⁾POI ARC approved baseline plan for 2019/20 (5 internal control reviews & 1 change assurance review).

Internal Audit reviews in progress and planned


3. The following reviews are in progress or being planned for delivery in Q4:

Post Office Ltd			
	Review	Status	Timing
1	Telco Billing Process	Reporting	04/11 - 25/11
2	HIH (Change)	Reporting	25/11 - 13/12
3	Branch Banking Framework	Fieldwork	08/01 - 24/01
4	Accounts Receivable	Fieldwork	13/01 - 31/01
5	Investment Funding Controls follow-up	Fieldwork	20/01 - 07/02
6	Data Privacy	Fieldwork	13/01 - 07/02
7	Supply Chain (CVIT)	Planning	Feb
8	Agent On-boarding	Not started	Feb
9	Vetting / Fit & Proper	Not started	Feb
10	SPO Controls (Phase 2)	Not started	Feb
11	Effectiveness of Compliance Function	Not started	March
12	FS Branch Sales	Not started	March
13	Savings Accounts (Sales)	Not started	March
Post Office Insurance			
14	Revenue Recognition	Planning	Feb
15	MI Platform	Planning	March



Internal Audit reviews completed

4. Since the November ARC meeting we have finalised the following 4 reviews:
 - PCI Programme
 - Cyber Security Follow-up
 - CFS Controls (Post BOT)
 - Third Party Oversight (POI)
5. Our findings and observations from these reviews are summarised below, with the full reports available in the reading room.

PCI Programme (Programme Assurance) (Ref. 2019/20-13)									
 <p>Needs Significant Improvement</p> <p>Sponsor: Shikha Hornsey</p> <p>Audit actions:</p> <table border="1"> <tr> <td>P1</td><td>2</td></tr> <tr> <td>P2</td><td>3</td></tr> <tr> <td>P3</td><td>1</td></tr> <tr> <td>Total</td><td>6</td></tr> </table>	P1	2	P2	3	P3	1	Total	6	<p>The PCI Programme was launched in November 2018 to regain compliance with the Payment Card Industry Data Security Standard. The programme is now in its 3rd iteration, having developed from a purely technical solution to update the Point-to-Point Encryption (P2PE) in the existing PIN Pads to a more holistic solution (per its most recent business case) that also addresses retail payments and the Banking Framework processes.</p> <p>The objective of this review was to assess the operating effectiveness of programme setup and delivery activities.</p> <p>While good work has been done since June 2019 in managing the programme activities and in driving a more holistic approach towards compliance, the programme carries a significant residual risk to Post Office's ability to achieve compliance. There is also a remaining inherent risk of non-compliance as a result of the late shift of compliance position and the scale and complexity of the remediation work that is now needed. The programme has been impacted by challenging relationships with third parties (most notably Fujitsu and Ingenico) as well as significant changes in Post Office leadership (having had 5 different sponsors in the current financial year).</p> <p>Whilst the full detail costs of the solution, including run costs are not yet agreed, the current forecasted spend exceeds the approved funding by £1.5m, with £880k of additional running costs and timeline to regain PCI compliance potentially being extended to end of Q1 2021.</p> <p>We highlight the following key issues that are within the control of the programme to address:</p> <ul style="list-style-type: none"> • Insufficient committed resources to support programme delivery; • Incomplete assessment of PAN data across Post Office; • Inability to fully demonstrate that the PCI guidelines were followed on the current proposed remediation.
P1	2								
P2	3								
P3	1								
Total	6								
<p>Management Comment provided by Shikha Hornsey</p> <p>The PCI Programme has been re-prioritised to become one of the Post Office's major initiatives. As such it is receiving much more focus, as well as more resources, to ensure that the Post Office's PCI compliant solution will be ready for deployment in December 2020. However, as the Christmas shopping period is typically the busiest time of year, it is expected that the actual software deployment of the compliant solution may roll out early in the first quarter of 2021 due to the Christmas freeze. All effort is being made to shorten that time line wherever possible in order to target a December 2020 compliance date.</p>									



Cyber Security Follow-up (Ref. 2019/20-17)



Sponsor:
Shikha Hornsey

Audit actions:

P1	0
P2	3
P3	1
Total	4

A comprehensive Cyber Security maturity assessment was undertaken by Deloitte between December 2018 and May 2019. The review covered 34 capabilities across four domains and concluded that Post Office has made significant progress in developing its IT and Information Security capabilities. However, maturity scores were found to be below the average for the Retail sector, FS sector and Post Office's target maturity. Deloitte made 224 recommendations to close these maturity gaps, which are implemented through 10 overarching actions. The objective of this follow-up review was to assess the progress made to track and implement the actions required to achieve target maturity, ahead of a second comprehensive review due in 2020.

Significant work has been undertaken since the Deloitte review to enhance the control environment and we believe that the agreed approach to remediation will result in maturity levels consistent with the current targets. Completion of remedial actions is currently at 60%, which is slightly behind schedule (65%), but in itself no cause for concern. However, we have highlighted some control weaknesses, which if not addressed, may prevent the business from achieving the maturity targets set for Cyber Security by March 2020.

Management Comment provided by Tony Jowett (CISO)

"I agree that good progress has been made towards enhancing Post Office's cyber maturity. We accept the findings and actions detailed in the report and will address them within the agreed timescales."

CFS Controls Post BOT (Ref. 2019/20-16)



Sponsor: *Al Cameron*

Audit actions:

P1	0
P2	6
P3	2
Total	8

The objective of this internal audit was to assess the design and operating effectiveness of the Financial Reporting Controls that changed when processes migrated from POLSAP to CFS. The audit covered 77 controls across 7 processes.

It is our view that the emphasis placed upon this work by Finance continues to ensure that the business maintains a good level of control over its financial reporting activities. The training and guidance provided by the Financial Controls Team in the run-up to BOT has paid dividends and has contributed to a considerable improvement in the standard of controls being operated. We conclude that the control activities in this area are effective, although largely manual in nature. The audit identified some opportunities for improvement, which will further strengthen the controls.

Management Comment

"As always, we welcome the input from internal audit and the report is a fair reflection of the status of the new post BOT controls. I'm pleased with the progress made in this area and the significant improvements made to the control environment as a result of the hard work during BOT. The findings are not concerning in nature, however they will be acted on swiftly to ensure the framework is robust and controls are operating effectively. Additionally we'll continue to strive towards developing a more automated (less manual) controls environment." (*Tom Lee – Financial Controller*)

"We appreciate the review as this is never an area where we will be complacent." (*Al Cameron – CFO*)

**POI: Third Party Oversight (Ref. 2019/20-04)**

Satisfactory

Sponsor: Ed Dutton

Audit actions:

P1	0
P2	1
P3	3
Total	4

Post Office Insurance has introduced a well-designed framework, clear policies and prescribed processes to effectively govern, monitor and manage third parties. The experiences leading to the termination of contract with a key provider, Travel Insurance Facilities (TIF), mid-2019 have informed the approach and there is a clear emphasis on alignment with POI brand values.

We noted that the intra-group services agreement with POL (MSA) is not currently covered by the framework and we recommend that such agreements be brought within the process.

Overall, third party oversight within POI has been rated satisfactory to reflect that, although the activity is not yet mature, no significant design or operating weaknesses were found, and it is on track to become embedded in BAU.

Management Comment provided by Russell Tavener

"We found this audit to be probing and challenging and accurately reflects the positive progress that has been made to enhance our supplier management approach.

The findings are reasonable and will be used to further improve the level of rigor POI now enforces within the selection and management of our supply chain. We also believe that this audit provides compelling evidence how PO Group could implement SRM in an efficient but effective manner, for which we can offer support and experience."

Status of Audit Actions

6. Audit actions are generally being completed on time. The movement and ageing of audit actions are shown in the table below.

Audit Action Status (POL):		Ageing:	
Open actions at last ARC	75	Open (not yet due)	54
Less: Actions closed in period	43	Overdue (<60 days)	2
Add: New actions in period	24	Overdue (>60 days)	0
Total open actions	56	Total open actions	56

7. The following two actions are currently overdue (less than 30 days):

Description of audit finding and Priority	Action Owners and Status Update
FS Training (Branch Sales) (GE owner: Owen Woodley; Due date 31/12/2019)	
P2 - There is no high-level document setting out the approach to FS branch sales training. Action: Coordinate a cross functional effort to develop, position and maintain an appropriate FS training policy.	Owner: Elizabeth Garside (prev. Ross Hunter) Progress has been made although the departure of the initial action owner has resulted in a delay. The action has been reallocated and is scheduled for completion by 31 Jan 2020.
Purchase to Pay (GE owner: Al Cameron; Due date 31/12/2019)	
P2 - Segregation of duties is not enforced in CFS for Accenture support users. Specifically, 11 users were able to raise and approve requisitions and modify master data. Action: Management will investigate what steps can be taken by Post Office to monitor Accenture access to CFS. This could potentially be addressed by Accenture sharing the Authorisation Object and Transactions Report currently being tested in the development environment.	Owner: Joy Lennon Action is progressing. Accenture roles have been reviewed to tighten access to CFS and it is likely that changes to master data or transactions raised by Accenture staff will be picked up as part of normal monitoring process. However, more robust monitoring mechanisms still need to be implemented – appropriate solution is being discussed with Accenture, who have indicated this will be completed by 31 Jan 2020.

11

Confidential

12



Appendix²

Central Risk

Appendix 1: RCC Post Office Enterprise Risks

Appendix 2: RCC Risk Heatmap and supporting comments

Appendix 3: RCC Change Portfolio

Internal Audit

Appendix 4: Internal audit plan

Appendix 5: CFS Controls (Post BOT)

Appendix 6: PCI Programme

Appendix 7: Cyber Security Follow-up

Compliance

Appendix 8: Compliance Dashboard (Nov 2019)

Appendix 9: Compliance Dashboard Summary of Trends (Nov 2019)

Appendix 10: FS Regulatory calendar

Appendix 11: Telecoms Regulatory calendar

² Appendices are accessible in the CoSec 'Reading Room'



Post Office Limited Audit, Risk and Compliance Committee Report

Title:	Cyber and Information Security Policy Summary Paper
Meeting Date:	28 th January 2020
Author:	Hazel Freeman (IT Security Business Partner) / Ehtsham Ali (Head of Cyber Security Compliance)
Sponsor:	Shikha Hornsey (Chief Information Officer)

Input Sought

Action Required: Noted	Recommend for Approval by the Audit, Risk and Compliance Committee
Previous Governance Oversight:	Previous versions of the policy have been presented to the Risk and Compliance Committee.

Executive Summary

Context:	This paper provides a summary of changes that have been made to the information and cyber security policies below as part of their annual review process for the Committee to consider
-----------------	--



Questions asked & addressed

1. Which policies were updated in this annual cycle review?
2. What updates were included and why?

Report

Which policies were updated in this annual cycle review?

3. In this review cycle 1 policy has been revised pending approval and 3 have been deprecated and merged.

Policy	Last Reviewed	Updates
Cyber and Information Security	December 20018	Covered in the paper below.
IT Security	May 2018	Deprecated and merged into Cyber and Information Security Policy.
Acceptable Use	September 2018	Deprecated and merged into Cyber and Information Security Policy.
Document Retention and Disposal	March 2018	Deprecated and merged into Cyber and Information Security Policy.

What updates were included and why?

4. The changes made are:
 - a. Consolidated the top level Cyber and Information Security policies into one, simplifying where staff need to go, to get the business intent on cyber and information security.
 - b. The policy suite is supplemented with Cyber and Information Security standards which cover the measurable controls.
 - c. Minimum control section has been updated to incorporate controls from the current IT Security, Acceptable Use and Document Retention and Disposal Policies.