POL00401628

Agenda

POST OFFICE LIMITED

Meeting:	Risk and Compliance Committee
Date:	14 January 2020
Time:	14.00 - 17.00
Location:	0.05 Cloak Lane, Finsbury Dials, 20 Finsbury Street, London, EC2Y 9AQ

Present:	**Regular Attendees:**
Alisdair Cameron (Chairman)	Johann Appel (Head of Internal Audit)
Nick Read (CEO)	Mark Baldock (Head of Risk)
Ben Foat (General Counsel)	Jonathan Hill (Compliance Director)
Shikha Hornsey (Chief Information Officer)	Tom Lee (Head of Finance, Financial Accounting and Controls)
Cathy Mayor (deputising for Debbie Smith)	David Parry (Senior Assistant Company Secretary)
Chrysanthy Pispinis (deputising for Owen Woodley)	Rob Wilkins (Portfolio Lead) - Item 3
	Tony Jowett (Chief Information Security Officer) – Items 4, 5
	Meredith Sharples (Director, Telecoms) – Item 6.4
	Barbara Brannon (Procurement Director) – Item 7
	Andrew Goddard (Managing Director, Payzone) – Item 8
	Mark Dixon (Head of Treasury, Tax & Insurance) – Item 9
	Dan Zinner (Chief Transformation Officer) – Item 10
	Sally Smith (Money Laundering Reporting Officer and Head of Financial Crime) – Item 11
	Tim Armit (Business Continuity Manager) – Item 12
Apologies:	
Debbie Smith (Chief Executive, Retail)	
Owen Woodley (Chief Executive, Financial Services, Telecoms and Identity, Group Marketing, and Group Digital & Innovation)	
Lisa Cherry (Group HR Director)	

Time		Item	Owner	Action
14:00	1.	Welcome & Conflicts of Interest	Chairman	Noting
	2.	Previous Meetings	Chairman	
		2.1 Minutes (07 November 2019)		Approval
		2.2 Action List		Discussion
14:05	3.	PCI-DSS Update – verbal update	Shikha Horney	Noting (onward submission to ARC)
14:15	4.	Cyber Security	Tony Jowett	Noting (onward submission to ARC)
14:25	5.	Policies for Approval		Noting (onward submission to ARC)
		5.1 Cyber and Information Security Policy	Tony Jowett	Approval
14:35	6.	Combined Risk, Compliance and Audit Update		
14:35		6.1 Risk Report	Mark Baldock	Noting (onward submission to ARC)
14:50		6.2 Compliance Report	Jonathan Hill	Noting (onward submission to ARC)

Strictly Confidential

POL00401628

POST OFFICE LIMITED

15.05		6.3	Audit Report	Johann Appel	Noting (onward submission to ARC)
15.20		6.4	PSD2 Implementation	Meredith Sharples	Noting (onward submission to ARC)
15.35	7.		Supplier Contracts out of Governance	Barbara Brannon	Noting
15.45	8.		Payzone Risk Report	Andrew Goddard	Noting (onward submission to ARC)
15.55	9.		Tax Update	Mark Dixon	Noting (onward submission to ARC)
16.05	10.		Transformation Office Changes update	Dan Zinner	Noting (onward submission to ARC)
16.20	11.		Money Laundering Reporting Officer Annual Report	Sally Smith	Noting (onward submission to ARC)
16.40	12.		Business Continuity Update	Tim Armit	Noting (onward submission to ARC)
16.50	13.		Review of draft Audit, Risk and Compliance Committee (ARC) meeting agenda 28 January 2020	Chairman	
16.55	14.		Any other Business	Chairman	

Next RCC Meeting: Tuesday, 10 March 2020 at 14.00 to 17.00 in 1.19 Wakefield, Finsbury Dials, 20 Finsbury Street, London, EC2Y 9AQ

POL00401628

2

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 7 November 2019 at 13.00 pm

Present:	Alisdair Cameron (Chair) (AC)	Chief Financial Officer
	Lisa Cherry (LC)	Group HR Director (Interim)
	Ben Foat (BF)	General Counsel
	Shikha Hornsey (SH)	Group Chief Information Officer
	Cathy Mayor (CM)	Finance Director, Retail (deputising for Debbie Smith)
	Chrysanthy Pispinis (CP)	Post Office Money Director (deputising for Owen Woodley)
In Attendance:	Johann Appel (JA)	Head of Internal Audit
	Jenny Ellwood (JE)	Risk Director
	Jonathan Hill (JH)	Compliance Director
	Tom Lee (TL)	Head of Finance, Financial Accounting and Controls
	David Parry (DP)	Senior Assistant Company Secretary
	Barbara Brannon (BB)	Procurement Director (item 3)
	Tony Jowett (TJ)	Chief Information Security Officer (item 4)
Apologies	Mark Davies, Group Communications, Brand & Corporate Affairs Director, Debbie Smith, Chief Executive, Retail, Owen Woodley, CE Financial Services & Telecoms	

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

1.1 AC opened the meeting. He requested papers be shortened, the minutes summarised, 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 3 September were **APPROVED**.

2.2 Progress on completion of actions as shown on the action log were **NOTED.**

3. Supplier Contracts out of Governance

3.1 The Committee noted the following significant contracts in the procurement pipeline:

3.2 **SSK** – this is an £800K annual support contract that continues to non-compliantly roll-over without a strategy and business case agreed to purchase new, replacement and updated SSK machines. AC requested a retail lead team decision is made to ensure the project does not continue to stall. — **Action: CM/ Marketing**

3.3 **Brands/RAPP** – this is an £1m contract extended in April 2019. Strategy, funding and a sourcing plan require agreement. To avoid stalling, AC advised IT & Marketing to agree a date for tender before the next RCC meeting in January 2020. — **Action: SH/ Marketing**

3.4 **Global Payments** – this is a £10m contract for retail and digital payments processing which is due to expire in May 2020. An extension will be required whilst POL tenders for, and migrates to a new provider. The business is indicating that a two year extension would be requested with contractual termination for convenience negotiated to allow movement to a new contract/new provider at its earliest convenience.

3.5 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.

4. PCI-DSS Update

POL00401628

4.1 SH advised that she had met with Ingenico in Paris, where they had expressed their challenges in dealing with the bespoke product POL required. She expected to receive final pricing and deadlines at the end of this week (08/11/2019) which would be circulated. **Action: SH**

4.2 Due to the devices in the field requiring a software update once the software had been accredited by QCS (Quality Control Systems), she did not expect compliance to be completed until Q1 2021. The software update would take a day at most to complete.

4.3 The Committee noted POL's bespoke solutions but advised the report should more clearly articulate the reason for the extension in compliance. It was noted that the banks and ARC had been advised compliance would be in December 2020.

5. Cyber Security

5.1 TJ reported he was relatively comfortable with the progress made in implementing the Deloitte audit recommendations, of the improved cyber security, and the improved approach to joiners movers and leavers. He had concerns with 3rd party disaster recovery testing and the culture of ineffective password controls being used on personal laptops, PCs and devices.

5.2 He advised he would like to test maturity with POL's systems and 3 rd party vendors by completing a major incident test such as a ransomware attack.

5.3 The following was **AGREED**: **Action:**

1. A major incident test be completed with findings reported to the Committee. **TJ**
2. Joiners/movers/leavers – to review whether contractors who no longer work for POL have been removed from POL emails and systems. **DZ/LC**
3. Joiners/movers/leavers - A routine cycle of checking third party access to be implemented. **TJ**
4. Joiners/movers/leavers - IA to review end to end process of joiners/mover/leavers as part of the 2020/2021 IA audit plan. **JA**

6. Combined Risk, Compliance and Audit Update

Risk

6.1 The top risks of PCI, IT Technology and Interruption, People, Business Continuity, Payzone and Brexit were noted. The following points were discussed.

6.2 **Payzone** (paragraph 1.6 of the report) - CM (as a Board member of Payzone) remarked that Payzone was happy with the risk framework/controls now in place and noted that Payzone had a dedicated POL risk partner.

6.3 **PCI Compliance** (paragraph 1.3 of the report) – the project remained "Red" overall against current plan. SH agreed with this observation.

6.4 **IDS Digital Identity** (paragraph 1.16 of the report) – the project is six months behind schedule [post meeting note JE – this project is now nine months behind schedule]. AC requested the wording be reviewed and questioned whether the project should be reviewed at the Investment Committee.

Compliance

6.5 The following points were raised:

6.6 **Review of Cookie approach** (paragraph 2.9 of the report) – recent ICO guidelines advised that companies could no longer rely on implied consent when placing ccokies on websites. JH advised this would reduce POL's ability to use customer data held. Expressed consent must now be given.

6.7 **National Lottery and scratch cards** (paragraph 2.26) – tighter controls have been introduced by the Gambling Commission regarding the sale of gambling products to vulnerable customers. An agreed approach with the National Lottery is required.

6.8 **Mystery Shopping** (paragraphs 2.33 – 2.34 of the report) – results continued to be poor, a stronger message to non-compliant sites is required. AC sought ways to improve standards. **To do: JH**

6.9 **Super Complaint** – AC sought and received an update of the current position. Pricing papers would be presented to GE in December and were being reviewed against Ofcom's fairness principles.

6.10 The Law and Trends forum continued to horizon scan for any legal/regulatory updates that may affect POL.

Internal Audit

6.11 The following points were raised:

6.12 **Purchase to Pay** – controls around POL spend management have improved, but it is still heavily manual and requires an upgrade.

6.13 **Payzone Control Environment –** the control environment has improved over the last year and is for purpose, however when looked at overall, the control environment "needs improvement".

6.14 **Data and Analytics Excellence (Programme Assurance) –** AC advised the management comment would be reviewed for clarity. **Action: AC/SH**

POL00401628

6.15 **SGEI Validation** – initial feedback/challenge from UKGI had now resolved.

6.16 The current audit plan was progressing well and on track.

7. Contract Management

7.1 As previously discussed in the meeting, the Committee recognised the importance of better contracts management and POL's obligations under the Public Contract Regulations 2015.

7.2 BF explained a contract management framework would be introduced to improve rigour using a decentralised model placing accountability on relationship managers for a contracts journey.

7.3 AC sought to understand whether appropriate funding had been approved, whether POL should introduce contract managers, and whether a discussion on cultural change should be held by GE before the framework was implemented.

7.4 CM also questioned whether contract management should be a work objective for senior managers as she did not believe this was an appropriate objective for senior managers.

7.5 It was **AGREED** a discussion on contract management would be held at GE. **Action: BF**

8. Accountable Person

8.1 AC explained that Nick Read, as the accountable person (AP) under the terms of the Her Majesty's Treasury's ("HMT's") Managing Public Money ("MPM") principles, was the person responsible for governance, decision making and financial management of POL. (They are deemed to have overall responsibility for POL and will be held accountable for performance and action.)

8.2 To provide assurance to ARC and the Government (should evidence be requested), AC advised that an annual report would be produced stating how POL's AP had met their obligations.

9. Accounting Overview

9.1 AC advised that consideration should be given to a new accounting presentation that reflected the changes in investment funding, aligned POL's strategic objectives and considered changes in future financial measures used for bonus.

9.2 The suggestion is to remove the two column format from the P&L within the ARA, and having 1 column for P&L with 1 line for exceptional spend. Trading Profit could still be retained as a financial metric, however given that investment funding is due to end in 2021 it is suggested there be a shift towards generation and availability of free cash flow for reinvestment as a key financial metric for bonus purposes.

9.3 In order to address the financial measure of bonus, metrics would need to be agreed with the Remuneration Committee.

10. GDPR

10.1 JH provided an update on GDPR implementation into POL and the requirements for POL to observe.

10.2 Contract remediation work continues with 88 requiring remediation and 13 deemed to be high risk. Funding has been requested to complete this by Q1 2020/21.

10.3 All customer complaints reported to the ICO have been managed with no further action taken to date against POL.

11. Policies for Approval

11.1 The following policies were recommended for Approval at ARC:

- Change Management Policy
- Protecting Personal Data Policy
- Risk Policy

12. Review of draft Audit, Risk and Compliance Committee meeting agenda

The draft ARC agenda for 25 November was **NOTED** and discussed.

13. Future meeting dates RCC and ARC 2020 - 2021

13.1 The meeting dates were noted.

The next scheduled RCC meeting is 14 January 2020.

14. Any other Business

There was no other business.

POL00401628

Post Office Limited Risk and Compliance Committee Actions
Updated: 08.01.20

REFERENCE	ACTION	ACTION OWNER	DUE DATE	STATUS	OPEN/CLOSED
RCC Meeting 07.11.19					
3.2 Supplier Contracts out of Governance	SSK – retail lead team decision required to ensure project does not stall.	CM/Marketing		In progress – subject to PSG funding.	Open
3.3 Supplier Contracts out of Governance	Brands/RAPP – Agree date for tender	SH/Marketing		In progress – subject to PSG funding.	Open
4.1 PCI-DSS Update	Circulate final pricing and deadlines document from Ingenico	SH	January 2020	In progress. Update to be provided in PCI-DSS verbal update.	Open
5.3 Cyber Security	A major incident test be completed with findings reported to the Committee.	TJ	January 2020	Update to be provided in Cyber Security update paper.	Open
5.3 Cyber Security	Joiners/movers/leavers – to review whether contractors who no longer work for POL have been removed from POL emails and systems.	DZ/LC	January 2020	A paper is to be presented to GE.	Open
5.3 Cyber Security	Joiners/movers/leavers - A routine cycle of checking third party access to be implemented.	TJ	January 2020	Update to be provided in the Cyber Security update paper.	Open
5.3 Cyber Security	Joiners/movers/leavers - IA to review end to end process of joiners/mover/leavers as part of the 2020/2021 IA audit plan.	JA		JML has been added to the 2020/2021 IA plan.	Open
6.14 Internal Audit	**Data and Analytics Excellence (Programme Assurance) –** AC advised the management comment would be reviewed for clarity.	AC/SH	25 November	Report Updated for ARC	To close
7.5 Contracts Management Framework	It was **AGREED** a discussion on contract management would be held at GE.	BF		Discussion held at GE.	To close

POL00401628

Post Office Limited Risk and Compliance Committee Action Log
Updated: 14.02.19

RCC Meeting 03.09.19					
5. Compliance	GDPR – Contracts To identify contracts requiring GDPR remediation, the majority of which are IT service contracts with no owner identified.	Barbara Brannon and Shikha Hornsey	November 2019	This is in train for completion by 31 March 2020.	Open

POL00401628

Post Office Limited
Risk & Compliance Committee Report

4

Title:	Cyber Security Strategy Update
Meeting Date:	14 January 2020
Author:	Tony Jowett, Chief Information Security Officer
Sponsor:	Shikha Hornsey, Group CIO

Input Sought

Action Required:	1. To note the status and plans regarding Joiners, Movers and Leavers 2. To note the status and plans regarding Cyber testing
Previous Governance Oversight:	Actions to report on the above topics occurred at the previous Risk and Compliance Committee (RCC) in November 2019.

Executive Summary

Context:	The effective management of the access and rights of people joining, moving within and leaving the Post Office is key to reducing Cyber risk. This has been encapsulated into the Joiners/Movers/Leavers (JML) Programme. At the previous RCC this issue was discussed and at a December GE meeting a request was made for CIO/CISO to come back with a view of status and plans for this area. 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.

POL00401628

Questions asked & addressed

1. What is the current status of joiners, movers and leavers (JML) processes within Post Office and what are the recommended plans to improve these?
2. What is the current status and plans regarding Cyber Security testing?

Report - JML

3. Good JML processes are necessary to ensure that the right people have access to the systems and data they need to do their jobs effectively. People require different privileges according to their role e.g., admin users, and this needs to be managed in conjunction with how long the privileges are granted. The lack of good JML creates opportunities for both internal and external attackers to gain access to our systems and to get around integrity-focused controls in key business processes. If JML is overly bureaucratic then people will find ways around it e.g., by sharing login credentials rather than registering for their own, which undermines good security practice.

4. JML processes control access to the following assets and processes:

    a. Data and systems – both in-house and third-party
    b. Buildings
    c. Training and on-boarding
    d. Salary and reward through payroll systems

5. For *Joiners*, the key requirement is timely and accurate access in line with their start date to ensure they are productive from day one.

6. For *Movers* within the organisation, the key requirement is to make sure that enhanced access and privileges from the old role do not transfer to the new one where they may not be required.

7. For *Leavers* then the access to all data, systems, buildings, training and payroll is terminated as close as possible to the final date of employment or, by default at 5:30pm on that date.

8. Within Post Office JML must apply to all populations that are brand-affecting, including Post Office, Payzone, Post Office Insurance, 3rd party websites and portals (Condecco, OneTrust etc) as well as all 3rd party vendors who manage our systems. In each of these areas there will be both permanent and contract staff who need to have their access controlled. Clearly, the approach to third parties will be different to in-house staff but the end result needs to be the same – well-managed JML.

9. Our target is to implement a JML regime that has the following characteristics:

    a. Complete in coverage
    b. Consistent in application across organisation types
    c. Role-based according to the needs of each position

POL00401628

d. Risk-based – so those who have privileged access to our critical systems will have more stringent controls then those who only have standard access
e. Automated as far as possible – manual processes introduce scope for error and gaps but as we mature they will be used for contingency purposes
f. Controlled across all Post Office entities and third parties rather than individual departments doing their own thing in isolation
g. Communicated and understood – line managers and staff need to be aware of their responsibilities and act on them

10. In 2017 an internal audit report revealed that there were several deficiencies in the Post Office approach to JML. The actions from this review are still valid and whilst some have been completed, others require a reenergised focus as part of this programme of activity. The summary of findings from this report is included for reference in Appendix 1. A follow-up audit is scheduled for May 2020.

11. Since the audit, there has been notable progress through a joint HR and IT project to automate JML for Permanent Staff by linking Success Factors and Active Directory (which controls access to our admin estate). In addition to this HR provides Cyber Security with a list of people in their notice period to enable enhanced monitoring of their activities by the Security Operations Centre.

12. Contractors within Post Office are managed by SPO who manually provide IT and building security with JML input data. SPO directly manage timesheets and payments to contractors.

13. At the moment, there is a lack of a consistent programme of recertification of access to key data and systems – normally privileged access to crown jewel systems is reconfirmed every 3-6 months with standard access being reconfirmed yearly. This will be addressed as the JML programme matures.

14. Within third parties there are various regimes in place. As the majority of our crown jewel data and systems are controlled by third parties, this area needs to be a priority focus for the JML.

15. Actions in the Short Term (1– 3 months) are:

a. Form a working group to provide overall governance across Post Office and ownership of the end to end process. Membership will include IT, HR, POI, Payzone, 3rd Party Vendors, back office automation, etc.
b. Establish clear roles and responsibilities with corresponding RACI matrix
c. Identification of system and data owners for critical systems
d. Engage with system owners for our critical systems and assets to provide access to and reporting from their privileged access systems – monthly report of who has privileged access to our critical systems. This will include 3rd party vendors.
e. Identify the problem - Development of a known issues register for JML for subsequent projects' activity to close off
f. Development of end to end processes across all Post Office entities

POL00401628

16. In the Medium Term – (3 months - 1 year)
    a. Initiate project to develop an automated Identity and Access Management (IAM) platform across all Post Office domains
    b. Introduce regular recertification of access to critical systems and data
    c. Development of metrics to show how well JML is working
    d. Expansion of two-factor authentication to support JML and IAM
    e. Development of a comprehensive IAM strategy for Post Office

17. Over the Longer Term (1-2 years)
    a. Establishment of identity and access management operational capability across all domains – this will cover all areas and all types of data access.

Report – Cyber Testing

18. 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.

19. Cyber testing provides the evidence that cyber defences are working well and helps identification of gaps.

20. 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

21. 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.

22. Red-team testing is invasive technical testing performed largely in secret by an external organisation. As far as possible (without actually 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.

23. 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.

24. 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.

POL00401628

Appendix 1 – JML Audit Report Findings - 2017

Summary of Findings

The table below provides a summary of the findings and their ratings:

	Finding	Rating*	Action Owner	Date
IAM-JML Governance				
Scope Area: Process Governance				
1	No overall IAM governance (e.g. no ownership of the end to end process, no process diagram)	P1	Jane Macleod	30.06.2017
2	IAM–JML access management responsibilities (RACI) and controls are not clearly and transparently defined	P1	Jane Macleod	30.06.2017
Scope Area: People training and awareness				
3	Line managers not well informed about their responsibilities regarding IAM-JML process	P2	Martin Kirke	31.05.2017
Access Rights Management				
Scope Area: Joiners' process				
4	No assurance that access rights are limited to a need to know basis	P1	Martin Kirke	31.12.2017
5	HR does not have a full overview of all parties working for PO (employees, contractors)	P2	Martin Kirke	31.12.2017
Scope Area: Movers' process				
6	No assurance that access rights are reviewed when someone moves role/function	P2	IAM/JML Work group	TBD by the Working Group
7	Periodical access reviews not in place (for LAN, share drives and all applications)	P1	IAM/JML Work group	TBD by the Working Group
Scope area: Leavers' process				
8	No assurance that leavers' access rights are removed (timely)	P1	IAM/JML workgroup	TBD by the Working Group
Scope Area: Data and System Owners				
9	Data and system owners have not been identified (responsibilities assigned)	P1	Jane MacLeod	31.12.2017
Scope Area: Policy				
10	Non-compliance with the access control standard/policy	P2	Jules Harris	31.12.2017

* P1 = High Priority, P2 = Medium Priority, P3 = Low Priority

POL00401628

Post Office Limited
Risk & Compliance Committee Report

Title:	Business Continuity and Resilience Update
Meeting Date:	14th January 2020
Author:	Tim Armit, Business Continuity Manager
Sponsor:	Shikha Hornsey, Group CIO

5

Input Sought

Action Required: Discussion	For Noting
Previous Governance Oversight:	

Executive Summary

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

POL00401628

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?

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

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

Report

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

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

7. 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.

8. 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.

9. 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.

10. 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.

POL00401628

11. 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.

12. The planning for a response to the GLO ruling and to the threat of RMG industrial action was inclusive of contingency responses, such as the pop-up Post Office mentioned earlier in this report. The GLO ruling had no operational impact and required no changes to normal business approaches. The Media response was also muted and needed no crisis response. 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.

13. 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.

14. 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.

15. 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.

16. 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.

Financial Impact

17. None directly but additional budget will be required to mediate risks.

Stakeholder Implications

18. 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.

Next Steps & Timelines

19. Focus on Horizon resilience levels and continue to develop alternative working practices.

POL00401628

20. Support IT in reviewing root cause analysis and ensuring operational mitigations continue to meet business needs.

21. Escalate the Post Office on wheels solution.

POL00401628

Post Office Limited
Risk & Compliance Committee Report

Title:	Risk & Compliance Committee Report
Meeting Date:	14 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

6

Input Sought

Action Required:	For 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:	**1.** RCC is asked to • note the key enterprise risks and what the business is doing to address these • approve the closure of the Group Litigation enterprise risk noting some elements of the residual risk will be managed at intermediate/business level • note the key intermediate/business risks and what the business is doing to address these • note the 2 emerging enterprise risks (Date Analytics and End of Life components) and what is being done to address these • note the latest position on Brexit • note the latest position on the implementation of the Post Office's Governance, Risk & Compliance tool (Archer) • note the status of the Change Portfolio and its current top portfolio risks and key delivery challenges **2.** note 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 **3.** note the progress being made with delivery of the Internal Audit programme and completion of audit actions

POL00401628

Risk

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

Enterprise Risks

1 The Post Office currently have 13 active enterprise risks. A complete list is provided at Appendix 1. Based on their current RAG scores, the key enterprise risks facing the business are as follows.

Payment Card Industry Security Standards (PCIDSS) (4:4)

2 Because some of the Post Office's IT 3rd party suppliers are not compliant with the latest PCIDSS, there is a risk payments processed within branch could incur debit/credit data loss. PCI remains a key risk and its High RAG is unchanged since November 2019. PCI is reporting red as the baselined plans and costs from Ingenico and Fujitsu for delivery of the solution are overdue. Final commercial agreements with Fujitsu/Ingenico, Computacenter and Vocalink are all under review by vendor management, legal and delivery teams. However recent developments indicate the programme is gradually moving towards a more positive position. 25,000 Pin Entry Devices (PEDs) are currently within the Post Office estate. Corrective actions have been put in place to ensure the programme will complete delivery of PEDs by April 2020. Reassurance by our partners has indicated the implementation of the P2Pe accredited 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.

Retail proposition (5:3)

3 Because some agents consider the Post Office too complex and costly (potentially exacerbated by increased costs associated with Brexit) there is a risk the Post Office's retail value proposition becomes unattractive to other retailers and does not attract new agents. Mitigations include securing higher retention rates for existing postmasters and attracting new ones. A recent increase to agents' remuneration should improve branch sustainability along with plans to roll out more automated kiosks across the agency network, creating staff efficiencies. An opening hour's policy review should provide flexibility, allowing operators to choose hours based on local demand. We are working with our multiple partners at a strategic level and are trialling new initiatives such as RPOS and Parcelshop. The Developing Capabilities programme is working to provide Area managers with the skills and tools to build trusted relationships with Postmasters.

Brexit (4:3)

4 Because of the UK's decision to leave the EU there is a risk the impending UK-EU Free-Trade Agreement (FTA) negotiations will have a generally detrimental impact to the Post Office's long-term strategy, operations and infrastructure. The latest position is provided at paragraphs 0 et seq.

Group Litigation (5:3)

5 Because of the long running Group Litigation between Post Office and a group of (mostly former) postmasters there was a risk the High Court's final judgement(s) would find against the former. Group Litigation concluded in December 2019 when both parties reached a comprehensive resolution in full and final settlement following several days of mediation. As a result, the High Court action is at an end. Whilst a linked judgment recognises improvements we have made (and that our current Horizon system is robust relative to comparable systems), it makes findings about previous versions of the system and past behaviours which further demonstrate the importance of the changes we must make in our business, particularly the ways in which we support our

POL00401628

postmasters. Importantly, the Post Office has made clear the need to reset our relationship with postmasters and has started the process to build a much better relationship with them. In light of this we consider **this specific risk can be closed** but note a residual risk (i.e. potential additional claims and associated legal action) will be articulated at intermediate/business level.

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

Text Relay

6 In March 2019 Ofcom opened an investigation into Post Office's compliance with General Condition C5.9 (applicable since October 2018). This required all telecommunication providers to charge customers no more than the cost of a standard call for using text relay services[1], and to apply a special tariff scheme to these calls in order to compensate those customers for the additional time required. Ofcom concluded, in September 2019, that the Post Office was non-compliant and said it would be levying a £0.250m fine albeit this would be subject to a 30% discount if the Post Office agreed to settle. The Post Office have agreed to settle and we are expecting a public statement from Ofcom to that effect by mid-January 2020. The associated Telco business risk has therefore been closed. Further details provided in Compliance section (see paragraph 20).

Business Continuity

7 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 IT business reliance for robustness of contingency plans in place. An associated business risk will be articulated as needed.

Payzone Risk Management Framework/Workplan

8 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)

[1] Text relay offers text-to-speech and speech-to-text translation services whereby a relay assistant in a call centre acts as an intermediary. This enables people with hearing /speech impairments to communicate with other people over the telephone. Ofcom approves text relay providers, and has set out minimum service standards.

POL00401628

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

9 There are 2 risks emerging in the IT space. The first is around Data Analytics (3:3) whereby because of the complexity encountered with 'big data' and the absence of a clear roadmap there is a risk the Post Office's key business data is not accurate or up to date, kept safe and secure, specific for its purpose nor adequate and only used for a legitimate business purpose.

10 A potential risk (4:3) has also been identified in that there are around 200 end-of life hardware and software components managed by our various 3rd party suppliers which, if not proactively addressed, could lead to increased IT security vulnerabilities, software incompatibility, issues of non-compliance, increasing operating costs, and poor performance and reduced service reliability. Potential mitigations include undertaking a complete assessment of these End of Life components to determine status and uploading the baselined position into Service Now to allow for proactive configuration management.

11 We will be undertaking a deep-dive on these 2 risks (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?

12 The Conservative party secured an 80 seat parliamentary majority as a result of the December 2019 General Election. This led to the Queen's Speech being introduced on 19 December and the Withdrawal (Agreement) Bill (WAB) passing 2nd reading in the Commons on 20 December when Parliament broke for Christmas recess. At this point the 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.

13 UK Whitehall Departments are now turning their attention to preparing for, and commencing, UK-EU Free-Trade Agreement negotiations with the EU. At the time of writing the objectives, scope and sequencing for these negotiations still need to be finalised on both the UK and EU sides.

14 The nature of the FTA negotiations (and their impact on Post Office) will be significantly influenced by the timeframe. There was Conservative manifesto pledge that the FTA implementation period will not extend beyond 31 December 2020. The deadline for agreeing any future extension with the EU is by 1 July 2020. This can be done once, for 1 or 2 years.

15 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).

POL00401628

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

16 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.

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

17 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.

18 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 to through the choice of DWP's replacement solution. Vulnerable customers could be left without easy access to legacy POCa balances as DWP's replacement voucher service will not allow balances to be transferred. Post Office working with DWP to find a resolution.
- Legal Entity Optimisation (Delivery & Overall Red RAG): Route to Dividend work completed. Articles of Association (AoA) and Framework Documentation in agreed form. Formal approval at PO, POI Board and Payzone Boards will take place between January and March 2020. A Change Request will be progressed through governance 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.

19 Appendix 3 provides a summary of the current key 'Platinum and Gold' change programmes and their current reporting status.

POL00401628

Compliance
Telecoms

Text Relay

20 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).

21 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.

22 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.

23 We expect Ofcom to publish a summary of its findings and the fine on its website in early January 2020. Group Communications are prepared for any enquiries.

Fairness

24 We gave Ofcom an update on our progress on Ofcom's Fairness commitments. Ofcom has informally suggested that we reconsider our approach to home movers as some home are vulnerable, such as those who are being forced out of rented accommodation or frequent movers. Ofcom also considers that customers who are out of contract for a length of time are also likely to be vulnerable. Ofcom would like to see some progress on Post Office's position on out of contract customers given the number of customers in this position. The Telecoms team is looking at its options.

PSD2 – Please refer to the separate PSD2 & Telecoms paper

25 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.

26 Most telcos seem to have concluded that the application and compliance costs of a full licence outweigh the benefits, as many have opted for the electronic communications exclusion (ECE) for now.

27 This is further complicated for Post Office as we are an Appointed Representative of POI, BoI and Capital One and it is likely that we could not be both an AR and hold a full payment institution licence, similar to the Consumer Credit Licence issue when it moved from the OFT to the FCA.

28 There is recognition, however, that this may be a holding position until there is greater clarity around what will be covered in practice and what the FCA will expect.

- On 23rd December 2019 the FCA wrote to telecoms industry bodies to remind them of the PSD2 obligations and setting out the FCA's expectations in more detail. These

POL00401628

now need to be reviewed by the whole industry as they may not be practical and are complicated at best.

29 Initial legal guidance on this was that PSD2 did not apply to Post Office Telecoms, but this was challenged as it was at odds with the rest of the industry. A further opinion said that the regulations did apply. This was confirmed when we asked both law firms to resolve the conflicting advice. New guidance confirming that PSD2 applied was obtained in February 2019.

30 As a result of the final guidance the Telecoms team was advised it needed to make changes. It has been reviewing options to make the necessary operational changes and register an exemption with the FCA. It has been working with its partners/suppliers (e.g., Fujitsu and Talk Talk) who have been unable to offer a wholesale billing solution to meet the regulations, therefore a retail billing solution is being implemented in Q4 2019/20.

31 We expect to register with the FCA for the ECE shortly. We are seeking legal advice on the best approach for this and any potential penalties that might apply given the PSD2 regulations required an ECE to be in place from January 2018.

Data Protection

Post Office use of Cookies on Internet and Apps

32 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.

33 Post Office current position is non-compliant with both the guidance and case law however is similar to the approach being adopted by many in similar markets. 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 will 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

34 Work has commenced on the Contracts Remediation as outlined previously. The outstanding contracts have been considered and categorised and prioritised against streamlined criteria with focus on risk to personal data.

35 The first set of packs for the contracts identified for 'deemed consent' will be issued the first week in January. Simultaneously the team will be contacting suppliers where contracts are deemed to be of Material High Risk to Post Office.

36 During the analysis stage of work undertaken a further 199 contracts were found to have been de-scoped form the project. These are for contracts that had either expired, had no personal data involved or were due for renewal within one year. Further analysis is underway of these contracts to ensure that they have been categorised correctly.

37 The programme is planned to conclude in July 2020.

Payzone BPUK:

38 An initial review of Payzone Bill Payment UK against the provisions of GDPR was completed in early December 2019. An initial status report has been provided to the Compliance Director for consideration.

39 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.

POL00401628

40 The DP team will be working with PZBP UK to introduce the necessary changes and updates in Q4.

Freedom of Information

41 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.

42 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

43 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.

44 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.

45 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

46 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".

47 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

48 See separate MLRO report

Regulatory updates

49 See separate MLRO report

External Threats

50 See separate MLRO report

Supply Chain Compliance

POL00401628

51 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.

52 The compliance team have conducted an end to end review of Supply Chain value stock processes (including scratch cards and stamps) and have identified a number of control gaps. The report is being finalised and will be issued to stakeholders in January 2020.

Financial Services

Mystery Shops

53 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.

54 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.

55 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

56 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

57 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

58 There is only one new combined policy being updated in this cycle combining Information Security, Cyber and Access.

59 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.

60 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.

POL00401628

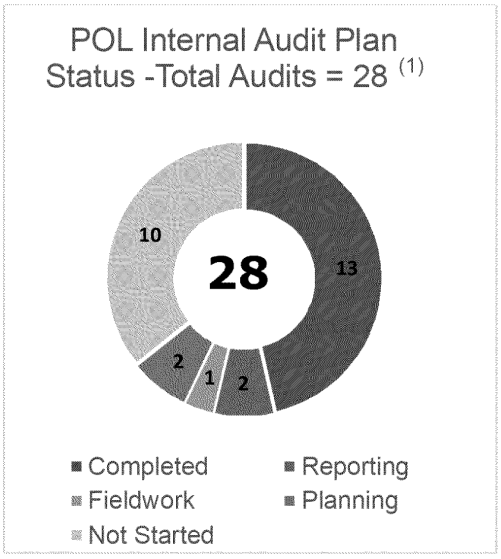
61 During 2019 with the temporary benefit of a Policy Manager we begun the work of rationalising the policy set from 125 policies to around 30 and ensuring that out of date policies were reviewed and approved. The current focus with the resources available is to work with policy owners in getting them to ensure policies are reviewed on time in the appropriate template.

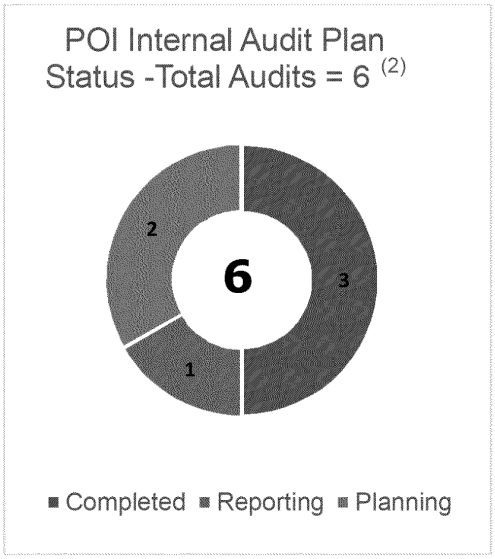
Internal Audit

Progress against plan

1. Delivery of the 2019/20 programme is making good progress, having finalised three more audits since the November ARC meeting.

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	Planning	08/01 – 24/01
4	Accounts Receivable	Fieldwork	13/01 - 31/01
5	Investment Funding Controls follow-up	Planning	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

POL00401628

Post Office Insurance			
14	Oversight of Third Parties	Reporting	Dec
15	Revenue Recognition	Planning	Feb
16	MI Platform	Planning	March

Internal Audit reviews completed

4. Since the November ARC meeting we have finalised the following 3 reviews:
   - PCI Programme
   - Cyber Security Follow-up
   - CFS Controls (Post BOT)

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)

Needs Significant Improvement

Sponsor:
Shikha Hornsey

Audit actions:

P1	2
P2	3
P3	1
Total	6

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.

The objective of this review was to assess the operating effectiveness of programme setup and delivery activities.

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).

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.

We highlight the following key issues that are within the control of the programme to address:

- 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.

Management Comment provided by Shikha Hornsey

The PCI Programme has been reprioritised 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.

POL00401628

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

Sponsor:
Shikha Hornsey

Audit actions:

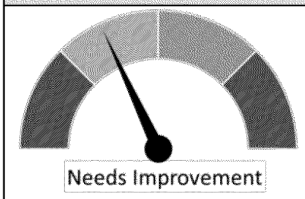
P1	0
P2	3
P3	1
Total	4

A comprehensive Cyber Security maturity assessment was undertake by Deloitte between December 2018 and May 2019. The review covere 34 capabilities across four domains and concluded that Post Office ha made significant progress in developing its IT and Information Security capabilities. However, maturity scores were found to be below th average for the Retail sector, FS sector and Post Office's targe maturity. Deloitte made 224 recommendations to close these maturit 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 th 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 th 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 maturit We accept the findings and actions detailed in the report and will address them within t 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 contro 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 the new post BOT controls. I'm pleased with the progress made in this area and the significan 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 robu and controls are operating effectively. Additionally we'll continue to strive towards developing a mo 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)*

POL00401628

Status of Audit Actions

6. Audit actions are generally being completed on time. Since the November ARC, 36 actions were completed and 8 new actions were added. As at 6 January there were 47 open actions, 3 of which were overdue.

Audit Action Status (POL):	
Open (not yet due)	44
Overdue (<60 days)	3
Overdue (>60 days)	0
Total	47

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

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 end 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.
Payzone Controls (GE owner: Debbie Smith; Due date 31/12/2019)	
P1 - Processes to support individual rights access requests and data breach reporting have not yet been defined and no link has been created between PZBP and POL for incident management. Action: Management will work with the POL Data Protection team to integrate processes for information requests, including Freedom of Information requests, and breach reporting.	*Owner: Michelle Embrey* Action is progressing. The data breach and information request processes are being developed in conjunction with the POL Data Protection Team. Chris Russell from POL DP Team has confirmed that engagement is in place, however, work required will take additional resource and will not be complete before 30/6/20.

POL00401628

Appendix[2]

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 RCC 'Reading Room'

POL00401628

Post Office Limited
Risk & Compliance Committee Report

Title:	PSD2 - Telecoms Implementation
Meeting Date:	14 January 2020
Author:	Meredith Sharples – Director of Telecoms
Sponsor:	Owen Woodley – CE, FSTI, Group Marketing, and Group Digital & Innovation

Input Sought

Action Required:	Noting
Previous Governance Oversight:	None

Executive Summary

Context:	This paper outlines the PSD2 implications to the Telecoms business and outlines the steps that have been taken by the Telecoms team to ensure compliance.

6

POL00401628

Questions asked & addressed

1. This noting paper provides the Committee with an update on the Payment Services Directive 2 ("PSD2") and the application of the regulations on our Telephony business.

What is PSD2 in relation to Telecoms companies?

2. PSD2 came into force for electronic communications companies in January 2018 in relation to billing customers for premium rate call services (e.g. Directory Enquiries and information services). The regulatory authority for PSD2 is the FCA. Telecoms companies had the option to either:

    - apply to register with the FCA as a payment provider and opt in for the full reporting regime; or
    - take an advantage of the Electronic Communications Exemption (the "ECE").

3. The ECE requires telecoms companies to cap premium rate service calls at £40 for a single call and cumulatively £240 in a monthly billing period. The ECE also requires the telecoms company to provide an independent audit, demonstrating compliance with the caps.

4. Most telecoms companies appear to have concluded that the application and compliance costs with the full reporting regime outweighs the benefits of not having to apply the caps, and have opted for the ECE.

Applicability of PSD2 on Post Office Telecoms

5. Following the creation of the Telecoms compliance function in early 2018, we joined an industry forum ("UKCTA"), where we were advised that PSD2, historically a payment services directive, might also apply to telecoms services. As a result we sought legal guidance from DAC Beachcroft in May 2018 on the relevance of the regulations to our telephony business.

6. The initial advice was that PSD2 did not apply to the Post Office Telecoms business. This was challenged by Compliance as it appeared to be at odds with the rest of the industry, most of whom had applied for an ECE. The risk that PSD2 did apply was added to the Telecoms risk register and raised at the RCC and ARC in July 2018.

7. Further legal advice was obtained from another law company (Linklaters) and in this instance the advice was that the regulations did apply to the telephony business. Because we had conflicting opinions from two companies we asked them to meet and resolve the conflicting advice. This was provided in February 2019 and confirmed that the regulations did apply and that Post Office, although not regulated by the FCA, was required to notify the FCA that it provides payment service. The Telecoms team was provided with this advice and asked to implement the changes required in order to comply with PSD2.

8. More recently, on 23rd December 2019 the FCA wrote to various telecoms industry bodies including UKCTA, asking them to remind their members of its expectations in relation to

POL00401628

PSD2. This may be because some telecoms companies may not have registered with the FCA or applied the ECE appropriately.

How will Post Office comply?

9. Regulatory notification: Post Office Telecoms is required to notify the FCA that it is seeking to rely on the ECE and will provide an annual independent audit report to demonstrate compliance.

10. Operational changes: The Telecoms team have been working with their suppliers to establish the optimal way to achieve compliance, the solution outlined below will require both immediate technical changes and ongoing business process changes to ensure compliance and monitor fraud.

Risks and Issues

Regulatory risks

11. The PSD2 regulations came into effect on 13th January 2018. As an existing telecoms provider, Post Office was required to notify the FCA that it provides payment service and that it will rely on the ECE prior to that date.

12. However, as set out above, Post Office only became aware of the relevance of PSD2 to the telecoms business in March 2018, when it joined UKCTA. Further, the PSD2 regulations explicitly state that whilst Post Office is subject to the PSD2 it is not regulated by the FCA. Legal clarification was sought and final advice was confirmed in February 2019.

13. As Post Office did not notify the FCA before 13th January 2018, has not been providing the FCA with the required reporting and it has not implemented a solution to cap the premium rate call charges, therefore there is a risk that the FCA could take action against Post Office and seek to impose a financial penalty on the business.

14. Linklaters has advised that it is unaware of the FCA applying any penalty in relation to PSD2 and telecoms to date and thus it is unknown what potential penalty range might be. However, the Telecoms team has been advised on what parameters the FCA will be taking into calculating any fines. Further investigation into quantum is being undertaken.

15. However, it may be that this area is not a priority for the FCA, hence its communication to the telecoms industry in December 2019, and that it might be satisfied, therefore will not apply any fines) if we notify for the ECE, implement the operational changes to apply the billing caps and, critically, ensure that any charges above the caps made from January 2018 have been refunded to customers.

16. The Telecoms, Compliance and Legal team are preparing a response to the FCA if further explanation is sought.

Financial Risks

17. To cap the cost of individual calls and monthly calls is not a simple task as it requires modifications to be made complex billing call rating systems. These systems were not designed to implement real time call rating, as rating is performed at the end of the period.

POL00401628

Therefore it is not technically possible to monitor calls in real time and terminate when it reaches £40.

18. To implement, the monthly cap requires the billing systems to continuously rate individual calls and apply a cap to the charge to the customer when it reaches £240. As real time rating is not available the only solution is to apply a cap retrospectively.

19. Any delay to the rating, and therefore implementation of caps, come with financial risk as the Post Office will still be required to pay the service provider the full amount of the call. For example if the uncapped call charge was £100 then Post Office would have to pay the service provider £100, cap the cost to the customer to £40 and absorb the £60 as a loss. Similar arrangements would apply for the monthly £240 cap.

20. The risk from fraudulent usage will be mitigated through fraud reporting on these call types. The current usage is considered low at £24k per annum, based on a 6 month sample of premium rate calls.

Remedial Actions and Next Steps

Implementing the billing system changes

21. Since the confirmation of the legal guidance in March 2019 on the applicability of PSD2 to the Telecoms business, the Telecoms development teams have been working to define a solution with our suppliers Fujitsu and TalkTalk. The solution analysis took longer than normal due to a large number of uncertainties during the period, but a compliant solution is now committed for delivery in Q4 19/20.

22. The PSD2 solution was included in business roadmap planning with Fujitsu within 5 days of the formal confirmation of legal advice in March 2019. The completion of the definition stage of this change was significantly complex due a number of uncertainties in the FCA guidance, differing industry implementation and uncertainty from the supplier on a compliant solution. Tasks completed during the implementation period included:

    - Legal points were addressed through further engagement with POL external legal advisors e.g. Consumer T&Cs changes to contract length (initially interpreted that POL would have to change all end user contracts to 6 months).
    - A wholesale solution from TalkTalk was explored but removed in November 2019, after an initial proposal from BT Wholesale offer (made in September 2019) was rescinded. We do not know why the BT offer was rescinded but it does indicate the changing and complex nature of this obligation.
    - Two separate compliant options are provided under the regulation (as outlined above), the business needed to review the wider implications of option 1.
    - In December 2019 a change request was formally submitted to Fujitsu.

23. The timeline to rectify is outlined below.

POL00401628

	2019										2020		
	March	April	May	June	July	August	September	October	November	December	January	February	March
Formal notification of compliance requirement	3												
Enters Roadmap planning with FJT	8												
End user T&Cs, legal guidance on 6m contract		26	25										
Solution Design/Evaluation													
BTW proposal on call capping (later rescinded)							10						
TT confrimated no wholesale solution									8				
Confirmation that "Option 2" not an option									28				
Final Change note agreed with Fujitsu										20			
Implementation													

Refunds for impacted customers

24. Any customer impacted for the period January 2018 through to the implementation of the new charging caps deployment date, will have a single aggregated ex. VAT credit applied to the customer bill. The credit calculation will use the same calculations described below for ensuring compliance moving forward.

25. Any individual calls made to premium rates services (numbers beginning 118 / 0843 / 0844 / 0845 / 0870 / 090) will be capped at £33.33 ex. VAT and presented on the customer bill accordingly.

26. The monthly aggregate of calls made to premium rates services will be capped to £200 ex. VAT. For customer with quarterly billing this calculation will be repeated for each month period in the quarter.

27. Supporting annual reporting will be provided demonstrating compliance.

Notifying the FCA

28. Following advice from Linklaters, it is proposed to notify the FCA and request an ECE as quickly as possible. Therefore, we propose to write to the FCA informing it that we are implementing the caps on customer charges and will be refunding customer any excess amounts incurred since 13th January 2018. We will also advise the FCA that we are seeking to rely on the ECE. A draft letter to the FCA is being finalised, which we expect to send on 14th January 2020.

29. Additionally, we are preparing our position should the FCA ask why the PSD2 obligations were not implemented in 2018.

POL00401628

POST OFFICE LIMITED
RISK COMMITTEE REPORT

Title:	Procurement Governance & Compliance Report
Meeting Date:	14th January 2020
Author:	Barbara Brannon, Procurement Director
Sponsor:	Alisdair Cameron, Chief Financial Officer

Input Sought

Action Required:	For Noting and Discussion if further action if required.
Previous Governance Oversight:	November 2019 - Quarterly Risk Report

Executive Summary

Context:	As a business in receipt of public funds POL is bound by the Public Contract Regulations (2015). PCR 2015 oblige POL to behave in a fair, objective & transparent way when contracting with 3rd party suppliers. Additionally, set procedures must be followed for spend above £25k and £181,302. The purpose of this report is to set out both breaches to Post Office governance and key controls around contracts and compliance to PCR regulation in the award of contracts. The aim of collating this information is to drive improvement in awareness and compliance behaviour across the organisation. The second and primary aim is to work with GE and Business Units to commence commercial reviews in a more timely way ensuring POL obtains value, commercial and contractual flexibility fitting the requirements and business strategy of the organisation.

POL00401628

Questions asked & addressed

1. *How many and what types of procurement non-compliance have occurred in the past quarter?*
   Since the last RCC report in November there have been 11 non-compliant incidents with a total value of £2,621,652.
   A list of these awards is set out at the beginning of Appendix 1.

2. *What are we doing about it?*

   Active reviews continue with Business Units with the highest values relating to non-compliance.

   Our overall non-compliance value has risen from £17.65m in November to £20.2m in January.

   This was primarily driven by new high value direct awards.

   A visual breakdown is available in Appendix 2.

3. *What is in the current Procurement pipeline which is high value and at risk of being awarded or extended non-compliantly?*

   a) £800k. **SSK support** - with NCR for 2020/21 will be required while POL goes to market for a new supplier. Strategy for building a compliant route to support legacy support is TBC. It may be more economical to extend current contract until current devices are end of life.

   b) £1m **Brands/Rapp** – this has been extended to April 2020. A business strategy, funding and sourcing plan needs to be agreed. This is due to be submitted to the PSG shortly and Procurement are working with the Marketing and IT teams to build the sourcing options available.

   c) £1.5m **Media Planning Contract** – ongoing discussion with Marketing team who have a preference to run an OJEU process. Current contract expires 30th April 2020 and an OJEU process is no longer achievable in the remaining timeframe. A 6-7 month non-compliant extension will be required. A CCS framework exists for this service however, while the pricing is competitive the incumbent provider to POL has not been appointed to the new panel.

   d) £10m **Global Payments** – continuous delays to the Crown Commercial tender process for the new framework will result in the new panel of providers being appointed in January+ 2020. At this point POL can commence its own tender process. The contract with the incumbent provider, Global Payments will end 8th May. POL will therefore need to extend this contract for 12/24 months to allow for a process to

POL00401628

be run and possible migration to a new provider. A paper goes to GE outlining the options in January 2020 which Procurement are currently inputting to.

e) An approved strategy to bring POL recruitment services/agencies into compliance is outstanding. This is due to be completed in January 2020 with a tender process commencing immediately. The aim is to put a compliant panel in place by 31st March absent a change in recruitment strategy by HR/POL Mgmt.

f) Identity Services – a paper is due to go to GE shortly outlining POL options to reprocure services which will end in November 2020.

Conclusion

Non-compliant awards of contracts are already subject to extensive internal governance, legal and risk review, in line with POL governance guidance on value and risk.

Individually, all large value non-compliant contracts have been reviewed by appropriate Post Office governance forums with agreement on next steps and actions towards remediation allocated where appropriate and/or available.

Executive support towards moving POL towards a more compliant footing is very strong, but equally as important there is extensive support towards the cultural change required to ensure that Procurement activities and outcomes will support longer term business strategies and we reduce commercial risk making our 3rd party arrangements fit for purpose.

Report

1. What are the potential consequences of non-compliant awards?
   a) Pre-contractual remedies overview: During a Procurement, an aggrieved party can seek an interim injunction suspending the tender or the implementation until the court decides on an outcome.
   b) Post-contractual remedies: The court can order an 'ineffectiveness order' rendering the contract void &/or can award damages.

2. Why are these incidents of non-compliance occurring, and what can be done about it?

   Non-compliant awards are made for a variety of reasons at the Post Office.

   a) Low value, time constrained or highly sensitive/specialist engagements are common.
   b) Large commercial arrangements cannot often be easily competed or unravelled without operational impact, and re-procurement may be subject to a pending evolution of a supporting Business Strategy.
   c) The contractual arrangements may pre-date PCR 2015 regulations or the contract novated during separation from RMG, automatically becoming non-compliant at the renewal point. Non-compliant awards are frequently made on a tactical basis to extend contractual services while public tender processes are executed.
   d) Delays to public sector panels of suppliers becoming available. The Post office makes extensive use of this low-cost route to market and new/refreshed panels are subject

POL00401628

to frequent delays from Crown Commercial Services. Single interim extensions [of periods under 12 months] while tender processes are run are considered to be low risk legally.

e) Changes in scope or value over the term of a contract may render the extension or renewal of services non-compliant. Material changes to the scope of a contract may render the whole contract non-compliant.

f) Disregard for, or lack of understanding of the regulations.

3. Why are we receiving this report?

A decision to collate this information into a single location was taken in the Autumn of 2016. The aim is to track and improve our overall compliance and commercial results as an organisation, while also ensuring perceptions are accurate. However, it should be noted that it will facilitate timely responses to Freedom of Information requests which adds risk to the Post Office commercial landscape.

4. Are any of these breaches arguable on regulatory grounds or are they all breaches?

A full explanation of the individual compliance breaches for direct awards over £181k [previously £164k] threshold is attached in Appendix A. Each entry details the nature of, and the value of the breach. The threshold is altered annually based on the FX rate between GBP and the Euro.

The Procurement Compliance Register does not at present give an indicative risk level attached to the award. This information is provided to the accountable executives under internal governance processes in the form of a PCR risk note before a contract above threshold is entered into, and if necessary, under Legal Privilege. In addition, all signatories to a contract have sight of the Risk note as part of the Contract Authorisation Form [CAF].

All entries are compliance breaches. A period of challenge applies to each PCR breach once an aggrieved party becomes aware or ought to have become aware. This risk finally expires at 6 years from the date of breach. The defensibility of a legal challenge is outlined within a Risk Note.

5. *How many of the breaches were approved in advance and how many retrospectively?*

9 out of 11 contracts entered into during this period were not compliant with internal governance processes on contract and commercial review. All were for awards of between £0 and £100,000k. It is assumed that the McKinsey engagements were discussed and funding approved in advance of engagement along with legal review on the terms and conditions of engagement.

6. *Why were the approvals given?*

The rationale for approval is relevant to the individual service and is detailed within Appendix C.

7. *What were the unapproved, material breaches?*

There were no unapproved, material breaches during this period.

POL00401628

8. Describe what you are doing about the breaches. Where we are in breach, do we have a plan to come back into compliance and over what time period will that plan take effect?

a) A forward view of material contracts falling under each Business Unit is currently prepared by the relevant Procurement Manager for discussions with their key stakeholders. The maturity of this look ahead view does vary currently and is consistently a high priority activity within the team.
b) Sourcing options papers are prepared for review by contract managers and key stakeholders [risk, legal, security] with routes to market agreed. In many cases these are dependent on evolving business and operating model strategies and the Procurement team are now actively involved with some units helping to advise and review options as thinking evolves.
c) Where a non-compliant award is proposed due to time pressure, Procurement are actively working on long term mitigation with awards made on an interim basis to meet urgent operational needs.
d) Each RCC member now receives a regular report on compliance within their business unit[s].
e) A new Risk & Governance process requires a Risk Exception report to be created for non-compliant direct awards with SLT or GE sign off.
f) All Professional Services engagements must be approved in writing in advance by the COO. A compliant panel of preferred consulting partners has been appointed and proposed engagements outside of this panel are subject to additional review and challenge.
g) Procurement provides training as part of the revised Induction process for new staff. Training packs are being updated for existing staff and a new training module made available on Successfactors. Ad hoc training sessions for interested Business Units are also run.
h) A new Intranet site has been launched for Procurement to improve visibility of process, regulation, and the panels of approved compliant suppliers available to POL business units.
i) A revised POL Procurement Policy and supporting processes is in progress giving more granular guidance.
j) Using Crown Commercial Services frameworks, panels of Preferred Suppliers are being refreshed and updated across a wide range of spend categories to reduce time to market, improve compliance and greatly improve commercial outcomes and legal risk.
k) A planned change to operational systems will, once live, give Procurement earlier visibility of potential compliance issues eg: contractual value thresholds.

Risk Assessment, Mitigations & Legal Implications

As a business in receipt of public funds POL is bound by the Public Contract Regulations (2015). PCR 2015 oblige POL to behave in a fair, objective & transparent way when contracting with 3rd party suppliers. Additionally, set procedures must be followed for spend above £25k and £181,302.

Failure to abide by the legislation or "slicing and dicing" contracts exposes POL to risk, both as far the commercial outcomes of the contracts as well as the reputational damage, legal remedies, censure & fines that can follow the discovery of a breach. Our compliance to PCR can be requested under a Freedom of Information request at any time.

The PCR Compliance Register allows for the tracking of breaches to PCR regulations at the Post Office and internal governance processes. One aim of collating this information is to drive

POL00401628

improvement in awareness and compliance behaviour across the organisation. The second and primary aim is to work with GE and Business Units to commence commercial reviews in a more timely way ensuring POL obtains value, commercial and contractual flexibility fitting the requirements and business strategy of the organisation.

Contract and financial governance policy and processes at Post Office are set by the Legal, Risk and Governance team with clear guidelines for staff availably on the Company Secretariat team intranet site. This sets out steps to be taken to obtain financial and contractual approvals prior to making a binding commitment to an external party. Non-compliance to internal governance processes are also captured within this report.

POL00401628

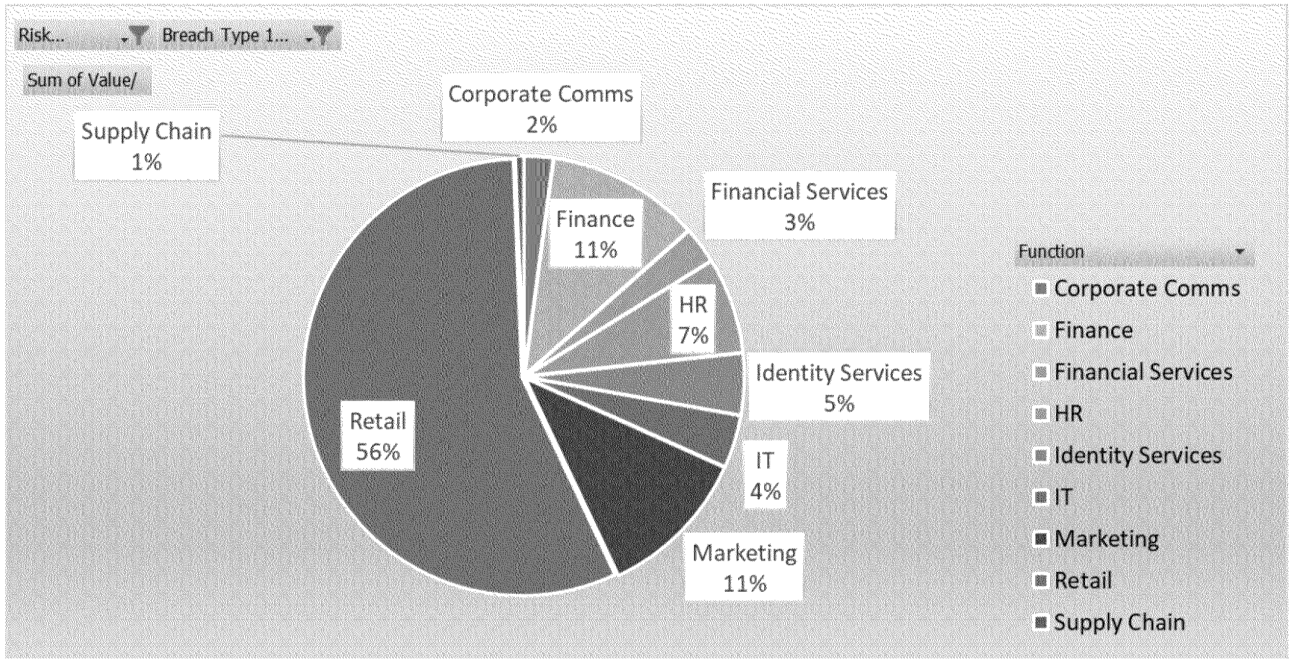
Appendix 1 - New Incidents over Reporting Period

Date	Purpose	Department	GE	Supplier	Value	PCR Compliant Y/N	Compliant POL Governance Y/N	Reason for engagement
18/11/2019	Employee benefits	HR	Lisa Cherry (interim)	BMI Healthcare	£ 15,000.00	N/A	No contract or CAF	Preference
16/12/2019	Management consultancy	Finance	Alisdair Cameron	Deloitte	£ 20,000.00	N/A	No contract or CAF	Employment Tax Support
16/12/2019	Marketing	Marketing	Mark Davies	Kantar	£ 24,500.00	N/A	No contract or CAF	Preference
14/11/2019	Management consultancy	Finance	Nick Read	McKinsey	£ 2,000,000.00	No	Approved Contract in Place	Preference
28/11/2019	Management consultancy	Finance	Nick Read	McKinsey	£ 250,000.00	No	Approved Contract in Place	Preference
23/12/2019	PR	Corporate Comms	Nick Read	Cardew Group	£ 78,000.00	No	Approved Contract in Place	Preference
30/12/2019	Digital Services	Retail	Debbie.K Smith	Abcomm	£ 42,000.00	No	Approved Contract in Place	Preference
30/12/2019	Digital Services	Retail	Debbie.K Smith	9XB	£ 30,000.00	No	Approved Contract in Place	Preference
30/12/2019	Comms, R&I & PR	Corporate Comms	Mark Davies	Kantar	£ 52,000.00	No	No contract or CAF	Preference
30/12/2019	Market Research	Corporate Comms	Mark Davies	AB Publishing	£ 100,000.00	No	No contract or CAF	Network Openings*
30/12/2019	Coaching/mentoring	HR	Lisa Cherry (interim)	Corrinne Projects	£ 10,152.00	N/A	No contract or CAF	Preference
				£	**2,621,652.00**			

POL00401628

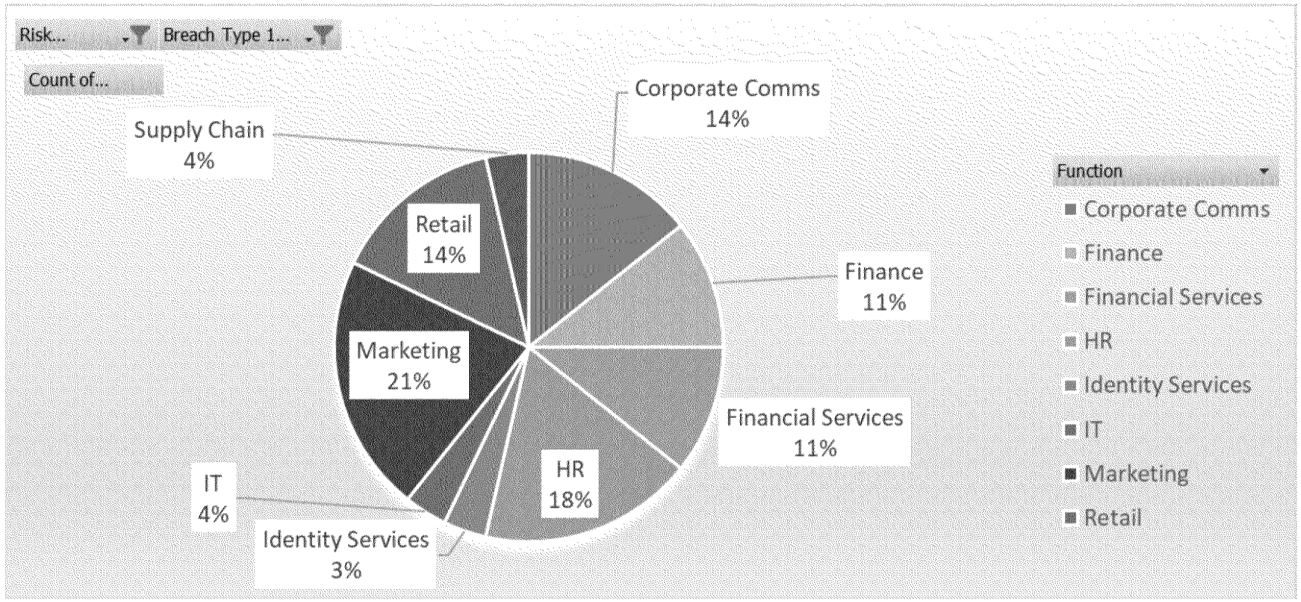
Appendix 2 – Breakdown of Open Non Compliant Risk by £/No.

Row Labels	Sum of Value/	
Corporate Comms	£	430,000.00
Finance	£	2,292,000.00
Financial Services	£	546,297.00
HR	£	1,429,500.00
Identity Services	£	920,000.00
IT	£	788,000.00
Marketing	£	2,273,440.00
Retail	£	11,392,000.00
Supply Chain	£	125,000.00
Grand Total	**£**	**20,196,237.00**



POL00401628

Row Labels	Count of Value/Incor
Corporate Comms	4
Finance	3
Financial Services	3
HR	5
Identity Services	1
IT	1
Marketing	6
Retail	4
Supply Chain	1
Grand Total	**28**



POL00401628

Post Office Limited
Risk & Compliance Committee Report

Title:	Payzone Bill Payments Update
Meeting Date:	14 January 2020
Author:	Michelle Embrey, Quality and Risk Manager, Payzone
Sponsor:	Andrew Goddard, Managing Director, Payzone

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 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 "pairing" issue affecting agent and customer transactions, and the risk to forecast revenues from under-performing. The progress of the risk framework from the previous reporting period includes the following: 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 process has been generated and submitted to POL risk team for their review and comments.

8

POL00401628

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 Panther RAID log
      (ii) Stage two, review the risks raised during the risk workshop held in July 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 risk work plan has been created that details all the key activities within the risk management remit. 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 Board. In Table 1, risks remain stable at 21. The financial risks have been reviewed and scored as 1 high, I medium, 3 low risk and 1 reassigned from the financial risk category to a legal, regulatory and other requirements risk category (from 5 blank).

POL00401628

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 the medium issues at 7 (decreased from 8).

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

8

b. **Significant Risks**

The top Payzone Bill Payments risks as shown in Appendix 1 are:

i **Risk score 20 (5:4)**
The urgency of the implementation for fixing the terminal pairing issue may increase with the onboarding of high-profile clients. This issue is currently under investigation and incremental software updates are released as improvements are established.

ii. **Risk score 16 (4:4)**
There is a need to consider GDPR requirements. Currently a formal process is being developed in conjunction with the Post Office Data Protection Team This risk has been given a high priority to mitigate and implement a process.

iii. **Risk Score 16 (4:4)**
The adoption and integration of the PO standards is an area of concern as the integration of the two businesses mature. Discussions are required to determine PO expectation of Payzone's level of standard implementation keeping in mind the need to maintain the highly dynamic and low margin operation. Also, discussions are required to ascertain where the risk of a reduced standard implementation would reside.

POL00401628

iv. **Risk score 15 (5:3)**
The risk to forecast revenues from under-performing against the original business plan. The success in securing the British Gas exclusive contract and pipeline of other key clients will mitigate this risk but there is need for further, detailed scrutiny on transaction and revenue growth.

v. **Risk score 16 (4:4)**
There is a risk regarding alignment of accounting and MI standards between POL and PZBP. This activity currently cannot be aligned due to the complexity of the POL systems and inconsistent data generated.

vi. **Risk Score 5 (5:1)**
Brexit has been scored as a potential black swan event.

7. **Conclusion**

a. There have been 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; the need to consider GDPR requirement the integration and impact of Post Office standards within operations and commercial areas, impact of Brexit, a terminal "pairing" issue affecting agent and customer transactions, and the risk to forecast revenues from under-performing (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.

POL00401628

Appendix 1

Significant Risks

Risk ID	Risk	Impact	Controls	Residual			Assigned To	Due Date	Progress Update
				Impact	Likelihood	Residual Risk Score			
RN021	Paring devices issue. Does this become a more urgent requirement to resolve	Unable to complete quantum transactions without reboot Customer impact as they maybe unable to purchase energy loss of merchants Reputational damage	Temporary work around is to reboot the equipment	4	5	20	RW	Dec-19	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 consequtive operation test and in readiness for 1st Jan exclusice service. Unlikely to release before mid January. Plan to be developed to communicate to retailers on resolution processs for pairin issue in order to reduce the impact to the helpdesk.
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	DS		(PRI026) 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 a 4 and likelihood also increased to 4 due to level of governance by PO & MSA no signed yet
RN024	Need to consider GDPR requirements for outbound sales calls, no formal process for holding data and removing data if requested	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, which ever is higher.	Controls in place include: Call recordings reports	4	4	16	KT	Mar-20	ME: Retention schedules created for HR, Helpdesk & Finance. Procedures 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
RN035	Risk around aligning accounting and MI standards between POL and PZBP, although PZBP can get down to a much more granular level than PO	This data is used as a base for business decisions. The alignment of accounting and MI becomes impossible due to the inconsistant of data from POL	Controls are currently being established	4	4	16	NS/POL	Mar-20	31.10.19 - NS: Work ongoing to improve collaboration between POL and PZBP in order to align MI
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	31.03.20	(PRI001) 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 bang on line with plan, costs lines greater. Statement from AG to Nicky which reflected this position. Chase her for this update. Technically the business isn't underperforming, costs are just greater 29/5/19-AG- Overall we're ok, from a P&L side we're spending more. Revenues on track, EBIT below. 26/03/2019 : PMO - Impact updated to 4 from 5.
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	Mar-20	(PRI001) 07.10.19 - (OP) 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 bang on line with plan, costs lines greater. Statement from AG to Nicky which reflected this position. Chase her for this update. Technically the business isn't underperforming,

POL00401628

Post Office Limited
Risk & Compliance Committee Report

Title:	Tax Update and Annual Tax Strategy
Meeting Date:	14 January 2020
Authors:	Mark Dixon, Head of Treasury, Tax & Insurance Andy Jamieson, Tax Manager
Sponsor:	Alisdair Cameron, Chief Financial Officer

Input Sought

Action Required:	The Risk and Compliance Committee is asked to note the Tax Update and the annual review of the Tax Strategy prior to submission to the ARC for approval.
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").

POL00401628

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 £1 billion over the period, approximately £3.5 million was paid to HMRC relating to two main issues, however approximately £5.5 million 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 c.£220m. RMG's VAT recovery positon was around 50% and, therefore, the VAT saving was c.£22m.

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.

POL00401628

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 £547k 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. 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. See para [28] for details.

IR35 – employment status of contractors

13. 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.

Deloitte review

14. 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 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

15. As at the 2017/18 tax year POL had accumulated tax losses of £843 million. We estimate that, once the 2018/19 tax computation has been finalised and submitted, POL will have losses carried forward of in excess of £900 million.

16. From April 2017 the tax loss carry forward that can be utilised is now restricted to an initial £5 million of profits and then 50% of the profits above £5 million. This means that POL will now begin to pay corporation tax sooner than it would have done under the old loss rules.

POL00401628

17. 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.

18. 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

19. In the October 2018 update we made the RCC/ARC aware of certain potential changes to the VAT treatment of commissions on bill payments.

20. Our bill payments business provides POL with approx. £25 million 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.

21. In 2017, following a VAT tribunal case involving PayPoint, HMRC queried whether we should apply the standard rate of VAT on all commissions.

22. 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.

23. 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.

24. 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 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.

25. 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. £1.5m 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.

Employees considered to have more than one permanent place of work

26. As indicated above, in 2019 we identified a number of employees who, under HMRC guidelines, could be deemed to have a permanent second place of work. We calculated that there was an underpayment of Benefit-in-kind ("BiK") tax of £254k, which was reported in the 18/19 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

POL00401628

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.

IR35 – employment status of contractors

27. As indicated above, 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.

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.

What other tax related issues should the RCC/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.

POL00401628

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.

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.

POL00401628

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.

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.

POL00401628

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.

Signed

Alisdair Cameron

Chief Financial Officer and Senior Accounting Officer

(Updated January 2020)

POL00401628

Post Office Limited
Risk and Compliance Committee Report

Title:	SPO Change Control Environment Update
Meeting Date:	14 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: *"A further update on the change control environment would be presented to the ARC in January 2020."* 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.

10

POL00401628

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

4. In terms of Finance controls, all CapEx and Exception spend (WBS codes) have limits set by central 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.

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. identify capable and competent resources to be placed on appropriately configured on teams;

POL00401628

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 **Appendix 2** and **Appendix 3** 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.

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. 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

POL00401628

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.

14. 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.

Stakeholder Implications

15. 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

16. 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
17. 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.

POL00401628

Appendix 1

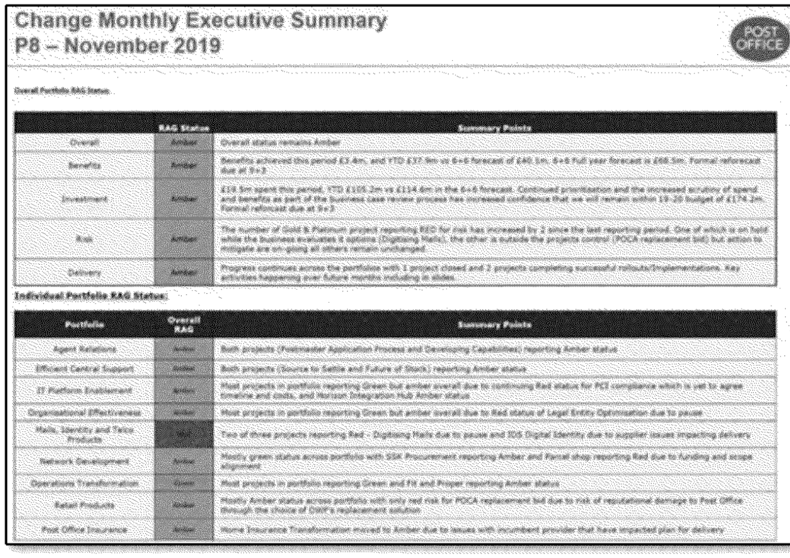
In September 2019, CTO's short term identified plan was to embed Change processes and ways of working through consistency, clarification and communication. The plan emphasised the immediate need to focus on the Change community first by increasing understanding on how to consistently manage and resource 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-assessement 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.

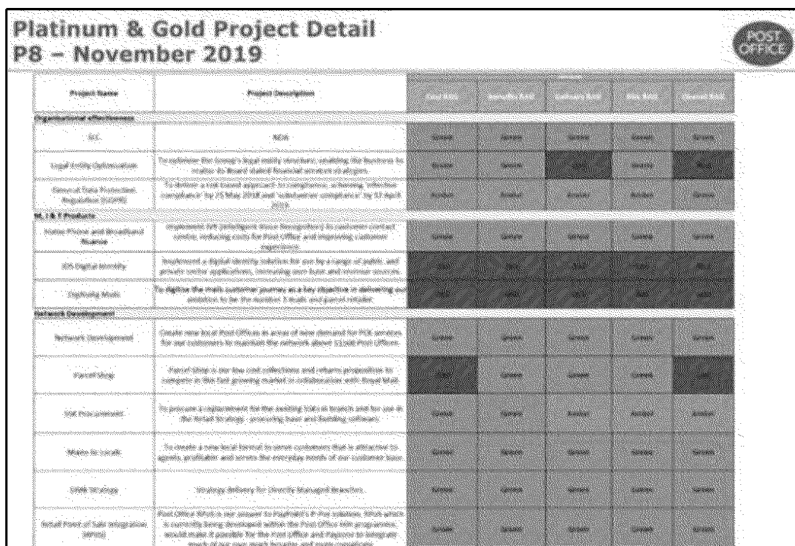
CTO FY19 Focus Areas		Progress to Date	Work to continue
People			
Structure fit for purpose Change teams		3 in SPO responsible for all skills pool resources (PM, PMO, BA)	Review all current project teams, starting with Gold/Plat, to ensure they are properly structured
Increase capable and affordable Change resources		50% contractors down from 62% YoY; £59k/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 heartbeart" 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 transparancy, 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 identfication
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

Appendix 2

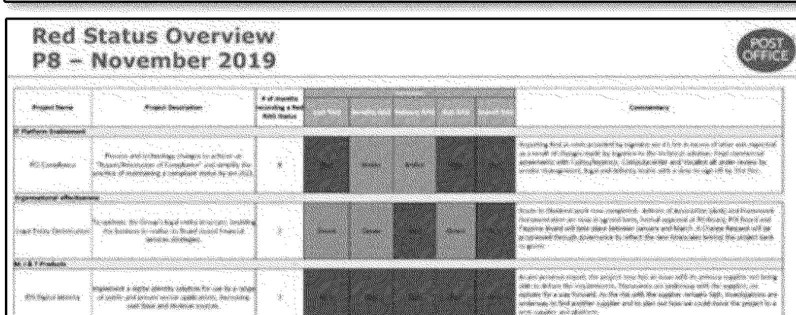
UKGI Monthly report provides the shareholder with a summary of the top (Platinum & Gold) programmes while at the same time allows the central SPO teams (risk, cross-portfolio, resource, and governance teams) a structured method to review and challenge projects on a monthly basis.



The report provides a summary of the entire Change Programme, as well as by portfolio. In addition, a summary of the monthly status for each Platinum and Gold programme is provided for 5 different areas (Cost, Benefits, Delivery, Risk and overall status).



If any project is "red" in any of the 5 areas, the SPO reports on the reasons for the "red rating." The SPO also challenges each programme monthly, regularly challenging any status based on weekly feedback from SPO teams.

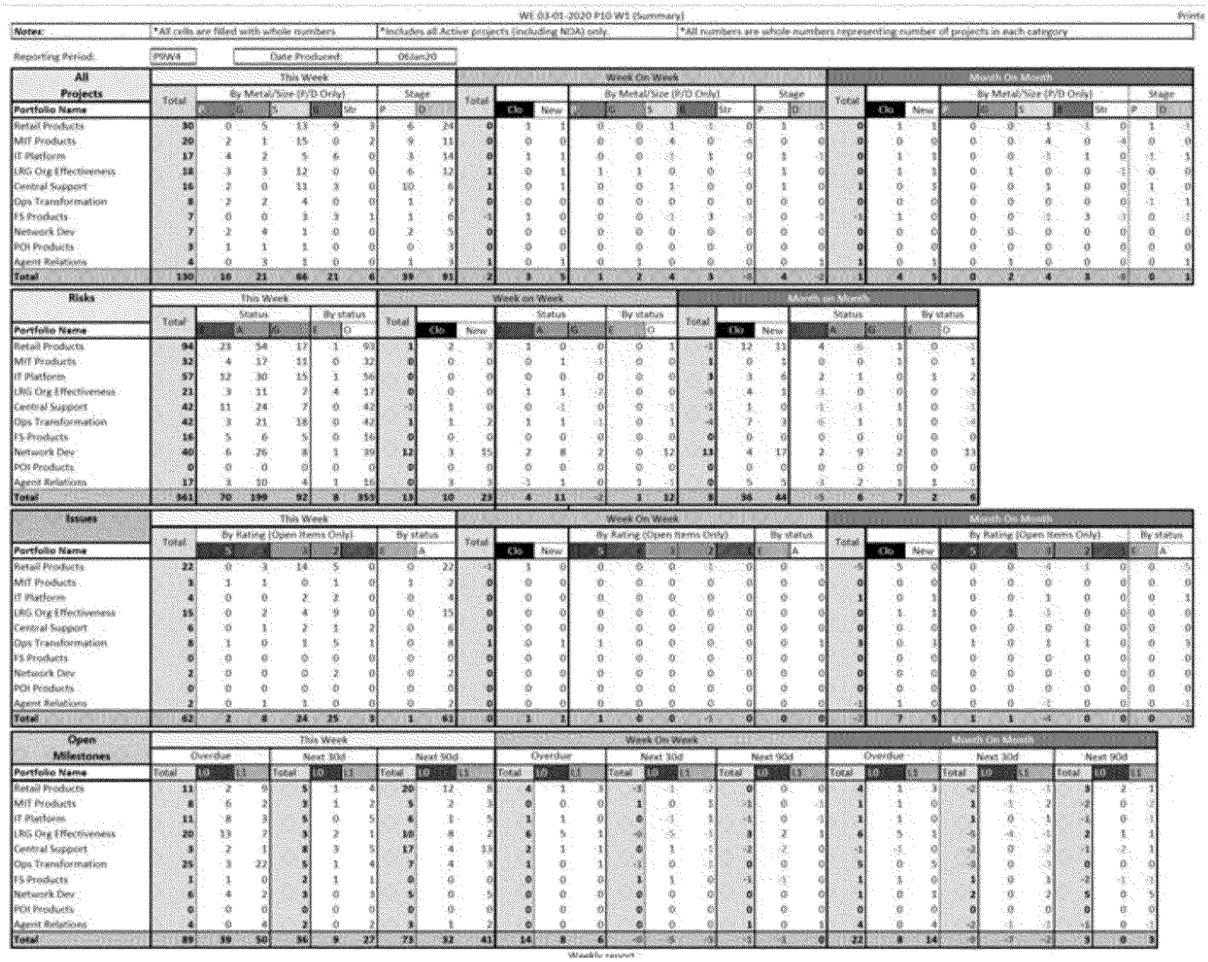


10

POL00401628

Appendix 3

Below is an example of the weekly Change Portfolio report provided to GE every Monday. The purpose of the weekly report is to highlight to GE members specific areas of concern (e.g., late milestones, open issues or risks, total size of the portfolio, data quality issues). While this report is created and provided weekly, the SPO is working on creating a means to systematically highlight areas of concern on a weekly basis. This is part of a programme to increase the data quality of project reporting in SNOW and to increase transparancy of the entire Change Portfolio.



WE 03-01-2020 P10 W1 (Summary)

Notes: *All cells are filled with whole numbers | *Includes all Active projects (including NOA) only | *All numbers are whole numbers representing number of projects in each category

Reporting Period: P9W4 | Date Produced: 06Jan20

All Projects

Portfolio Name	This Week Total	By Metal/Size (P/D Only) C	G	S		Str	Stage P	D	Week On Week Total	Clo	New	By Metal/Size (P/D Only) C	G	S		Str	Stage P	D	Month On Month Total	Clo	New	By Metal/Size (P/D Only) C	G	S		Str	Stage P	D
Retail Products	30	0	5	13	9	3	6	24	0	1	1	0	0	1	-1	0	1	-1	0	1	1	0	0	1	-1	0	1	-1
MIT Products	20	2	1	15	0	2	9	11	0	0	0	0	0	4	0	-4	0	0	0	0	0	0	0	4	0	-4	0	0
IT Platform	17	4	2	5	6	0	3	14	0	1	1	0	0	-1	1	0	1	-1	0	1	1	0	0	-1	1	0	-1	1
LRG Org Effectiveness	18	3	3	12	0	0	6	12	1	0	1	1	1	0	0	-1	1	0	0	1	1	0	0	1	0	-1	0	0
Central Support	16	2	0	11	3	0	10	6	1	0	1	0	0	1	0	0	1	0	1	0	1	0	0	1	0	0	1	0
Ops Transformation	8	2	2	4	0	0	1	7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	-1	1
FS Products	7	0	0	3	3	1	1	6	-1	1	0	0	0	-1	1	-1	0	-1	-1	1	0	0	0	-1	1	-1	0	-1
Network Dev	7	2	4	1	0	0	2	5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
POI Products	3	1	1	1	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Agent Relations	4	0	3	1	0	0	1	3	1	0	1	0	0	1	0	0	1	0	1	0	1	0	0	1	0	0	0	1
Total	130	16	21	66	21	6	39	91	2	3	5	1	2	4	3	-8	4	-2	1	4	5	0	2	4	3	-8	0	1

Risks

Portfolio Name	This Week Total	Status R	A	G		By status E	O	Week on Week Total	Clo	New	Status R	A	G		By status E	O	Month on Month Total	Clo	New	Status R	A	G		By status E	O
Retail Products	94	23	54	17	1	93	1	2	1	0	0	0	1	-1	12	11	4	-6	1	0	-1							
MIT Products	32	4	17	11	0	32	0	0	0	1	-1	0	0	1	0	1	0	0	1	0	1							
IT Platform	57	12	30	15	1	56	0	0	0	0	0	0	0	1	3	-2	2	1	0	1	2							
LRG Org Effectiveness	21	3	11	2	4	17	0	0	1	1	-2	0	0	-1	4	-3	0	0	0	0	-3							
Central Support	42	11	24	7	0	42	-1	1	0	0	-1	0	0	-1	1	-2	-1	-1	1	0	-3							
Ops Transformation	42	3	21	18	0	42	1	1	2	1	1	-1	0	1	-4	7	3	-6	1	1	-6							
FS Products	16	5	6	5	0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0							
Network Dev	40	6	26	8	1	39	12	3	15	2	8	2	0	12	13	4	17	2	9	2	0	13						
POI Products	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0							
Agent Relations	17	3	10	4	1	16	0	3	3	-1	1	0	1	-1	0	5	5	-1	2	1	-1							
Total	361	70	199	92	8	355	13	10	23	4	11	-2	1	12	9	36	44	-5	6	7	2	6						

Issues

Portfolio Name	This Week Total	By Rating (Open Items Only) 5			2		By status E	A	Week On Week Total	Clo	New	By Rating (Open Items Only) 5			2		By status E	A	Month On Month Total	Clo	New	By Rating (Open Items Only) 5			2		By status E	A
Retail Products	22	0	3	14	5	0	0	22	-1	1	0	0	0	0	-1	0	0	-1	-5	5	0	0	0	-4	-1	0	0	-5
MIT Products	3	1	1	0	1	0	1	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
IT Platform	4	0	0	2	2	0	0	4	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	1	0	0	0	1
LRG Org Effectiveness	15	0	2	4	9	0	0	15	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	-1	0	0	0	0
Central Support	6	0	1	2	1	2	0	6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Ops Transformation	8	1	0	1	5	1	0	8	1	0	1	1	0	0	0	0	0	1	3	0	3	1	0	1	1	0	0	3
FS Products	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Network Dev	2	0	0	0	2	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
POI Products	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Agent Relations	2	0	1	1	0	0	0	2	0	0	0	0	0	0	0	0	0	0	-1	1	0	0	0	-1	0	0	0	-1
Total	62	2	8	24	25	3	1	61	0	1	1	1	0	0	-1	0	0	0	-7	7	5	1	1	-4	0	0	0	-1

Open Milestones

Portfolio Name	This Week Overdue Total	L0	L1	Next 30d Total	L0	L1	Next 90d Total	L0	L1	Week On Week Overdue Total	L0	L1	Next 30d Total	L0	L1	Next 90d Total	L0	L1	Month On Month Overdue Total	L0	L1	Next 30d Total	L0	L1	Next 90d Total	L0	L1
Retail Products	11	2	9	5	1	4	20	12	8	4	1	3	-1	-1	-1	0	0	0	4	1	3	-2	-1	-1	3	2	1
MIT Products	8	6	2	3	1	2	5	2	3	0	0	0	1	0	1	-1	0	-1	1	1	0	1	-1	2	-2	0	-2
IT Platform	11	8	3	5	0	5	6	1	5	1	1	0	0	-1	1	-1	0	-1	1	1	0	1	0	1	-1	0	-1
LRG Org Effectiveness	20	13	7	3	2	1	10	8	2	6	5	1	-6	-5	-1	3	2	1	6	5	1	-5	-4	-1	2	1	1
Central Support	3	2	1	8	3	5	17	4	13	2	1	1	0	1	-1	-2	-2	0	-1	-1	0	-2	0	-2	-1	-2	1
Ops Transformation	25	3	22	5	1	4	7	4	3	1	0	1	-1	0	-1	0	0	0	5	0	5	-3	0	-3	0	0	0
FS Products	1	1	0	2	1	1	0	0	0	0	0	0	1	1	0	-1	-1	0	1	1	0	1	0	1	-2	-1	-1
Network Dev	6	4	2	3	0	3	5	0	5	0	0	0	0	0	0	0	0	0	1	0	1	2	0	2	5	0	5
POI Products	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Agent Relations	4	0	4	2	0	2	3	1	2	0	0	0	0	0	0	1	0	1	4	0	4	-2	-1	-1	-1	0	-1
Total	89	39	50	36	9	27	73	32	41	14	8	6	-6	-5	-1	-1	-1	0	22	8	14	-4	-3	-2	3	0	3

Weekly report

10

POL00401628

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE REPORT

Title:	Money Laundering Reporting Officer Annual Report
Meeting Date:	14th January 2020
Author:	Sally Smith
Sponsor:	Ben Foat

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.

11

POL00401628

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 c.£1.1m 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 c.£273m of fines have been levied by UK regulators in 2019. Additionally, HMRC annual registration fees have increased significantly from £1.4m in 2018 to £3.2m 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.
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

POL00401628

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 has delayed publication of the draft UK legislation relating to the Fifth Money Laundering Directive, 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.

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.

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

POL00401628

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.

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 and further work will be undertaken 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, and 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.

POL00401628

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	DCoE	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
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	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

* Assumes 10th January publication

POL00401628

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

11

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.

POL00401628

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 £796,500 in respect of premises registration errors, and £344,766 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 c. £273m 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).*

POL00401628

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.

POL00401628

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.

POL00401628

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 has[1]

- **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 ligation 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

POL00401628

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

POL00401628

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

POL00401628

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

POL00401628

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).

POL00401628

- 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.

POL00401628

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 £130 to £300 per annum with effect from 1st May 2019 meaning our annual registration fee for 1st

POL00401628

June 2019 was £3,197,400, reflecting the 131% 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 £100 to £150, 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

POL00401628

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

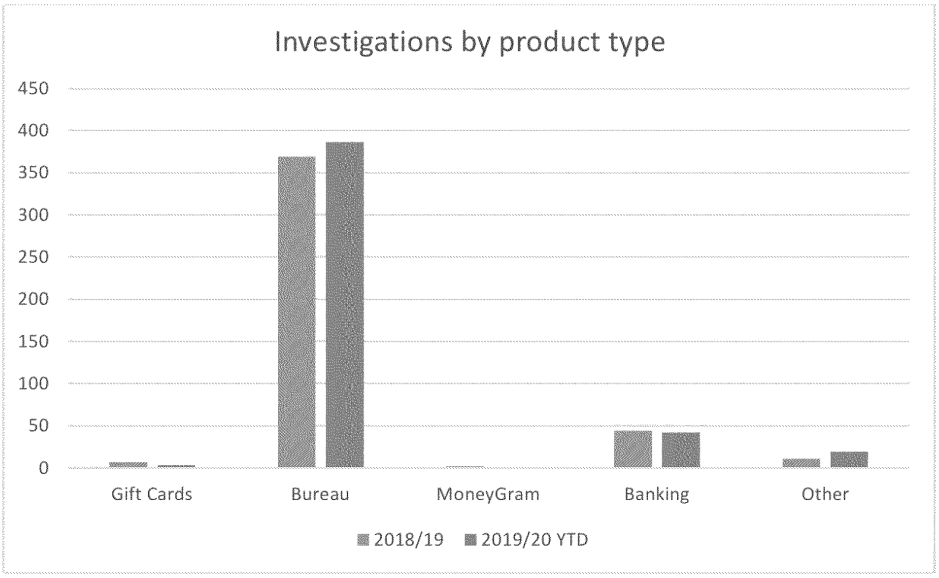
62. There have been 451 investigations up to P8 2019/20 (an average of 56 per month), this is compared to 433 for the whole of 2018/19 (an average of 36 per month). As detailed in the table below, the level of Bureau de Change investigations has already surpassed the number of investigations during 2018/19.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

POL00401628

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 8.6m & £2.46bn, and to P8 2019/20 6.1m & £1.73bn).

- 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.

POL00401628

- 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 2.7m & £807m, receive transactions 375k & £133m. Volume and value to P8 19/20: send transactions 1.6m & £485m, receive transactions 226k & £84m).

- 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 c.£92m compared to c.£32.2m 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 c.£39m, 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:

POL00401628

- 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. <u>One4All Gift Cards (GVS)</u> – 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

POL00401628

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

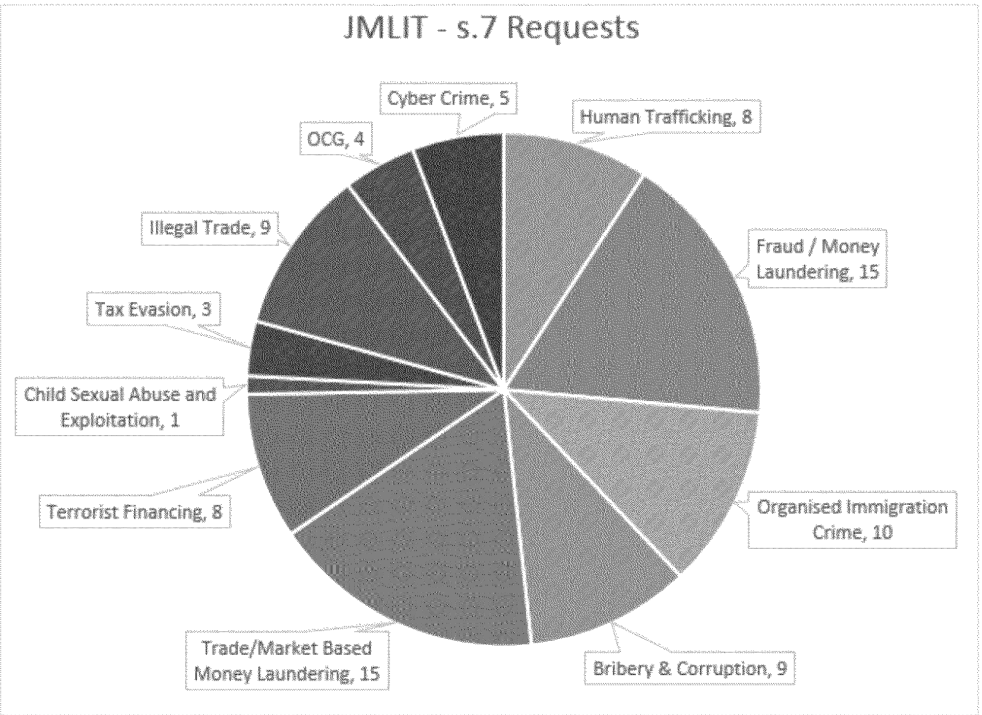
69. Card Fraud over Post Office counters – Between 1st January 2019 to 15th November 2019 there were 2122 fraudulent transactions processed to the value of £228,519.64; with the majority of transactions over £100 relating to Gift Card purchases. Card fraud has declined compared to last year, where there were 3,009 transactions totalling £425,635.35. YTD there have been no Card Scheme breaches.

70. The volume of JMLIT s.7[2] 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.*

POL00401628



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

POL00401628

- 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

POL00401628

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.

POL00401628

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

POL00401628

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.

POL00401628

Post Office Limited
Risk and Compliance Committee Report

Title:	Cyber and Information Security Policy Summary Paper
Meeting Date:	14th 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 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

12

POL00401628

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.

POL00401628

GROUP POLICIES

Cyber and Information Security Policy

Version – V2.0

12

POL00401628

12

POL00401628

1. Overview

1.1. Introduction by the Policy Owner

Post Office is committed to protecting its employees, customers, Third Party Supply Chain and information assets from damaging or illegal actions by individuals, either knowingly or unknowingly. Post Office enables this through the development and deployment of policies, standards and guidelines which are aligned to international best practices. Effective cyber and information security is a team effort involving everyone in Post Office.

1.2. Risk Appetite

There follows a list of applicable Risk Appetite statements for this policy:

- **Averse risk appetite** in relation to not complying with law and regulations or deviation from its business conduct standards, of which this standard forms part.
- **Averse risk appetite** in relation to any serious impact to the confidentiality, integrity and availability of information, leading to financial loss, business disruption, public embarrassment or legal consequences in line with risk impacts.
- **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 unethical behaviour including staff misfeasance.
- **Averse risk appetite** for data loss/leakage that can lead to customer, commercial or reputational damage
- **Neutral risk appetite** for operational IT services.
- **Averse appetite** for inaccurate and unreliable processing of data.
- **Averse risk appetite** for inefficient or ineffective or prolonged failure of, governance and control processes, critical financial reporting processes, critical supply chain and business continuity processes.

Post Office acknowledges however that in certain scenarios even after extensive controls have been implemented a risk may still sit outside the agreed Risk Appetite. In exceptional circumstances a Risk Exemption waiver may be granted

1.3. Purpose

The purpose of this is to detail the minimum IT controls required to reduce the Post Offices exposure to information security threats such as:

- threats from the internet (cyber threat)
- threats from internal staff (either malicious or accidental)
- threats from third parties (either malicious or accidental)

1.4. Core Principles

Compliance with this policy will ensure that the following principles are met:

POL00401628

- External suppliers to be identified and categorised such that a risk based approach can be facilitated in assessing the suppliers security controls.
- Security arrangements can be agreed and embedded into service agreements and contracts.
- Security controls can be validated prior to services commencing and on an ongoing basis.
- Termination of third party relationships can be effectively managed so as not to expose Post Office to additional Risks.

1.5. Application

This policy relates to all Post Office information assets, including critical business information systems, as defined by Post Office, and as amended from time to time, and applies to all employees[1]

Post Office information assets and systems include, but are not limited to:

- Business environments;
- Business processes;
- Business applications (including those under development);
- Information systems; and
- Networks

1.6. Legislation

Post Office seek to comply withall relevant UK legislation and regulatory requirements including (but not limited to):

- Data Protection Act (2018).
- Freedom of Information Act (2000).
- Privacy and Electronic Communication Act (2003).
- Regulation of Investigatory Powers Act (RIPA) (2000).
- Copyright, Designs and Patents Act (1988).
- Computer Misuse Act (1990).
- Human Rights Act (1998).
- Terrorism Act (2006).
- Limitation Act (1980).
- Malicious Communication Act 1988).
- Digital Economy Act (2010).
- Privacy and Electronic Communications (EC Directive) (Amendment) Regulations (2011).
- Counter-Terrorism and Security Act (2015).

[1] In this policy employee means employees permanent employees, temporary including agency employees, contractors, consultants and anyone else working on behalf of Post Office.

POL00401628

1.7. Industry Guidance

Post Office is a member of the Information Security Forum (ISF) which is used to p rovide input to Information Protection and Assurance (IPA) and IT Security developments.

1.8. Policy Framework

This policy forms part of the IPA and IT Security Policy Set which is located here:

https://poluk.sharepoint.com/sites/postoffice/inside/Pages/Information -security.aspx

1.9. Who must comply?

Compliance with this policy is mandatory for all Post O ffice services. All third parties who do business with Post Office, including consultants, suppliers and business and franchise partners, will be required to agree contractually to this standard or have their own equivalent policy.

POL00401628

2. Minimum Controls

A minimum control is an activity which must be in place in order to manage the associated risks within Risk Appetite. To be able to demonstrate compliance, mechanisms must be in place within each business unit or product to demonstrate complianc e. The minimum controls can cover a range of control types, i.e. directive, detective, corrective and preventive which are required to ensure risks are managed to an acceptable level and within the defined Risk Appetite.

The table below sets out the relationships between identified risk, and the required minimum controls. The subsequent page defines in greater detail terms used:

Risk Area	Description of Risk	Minimum Control	Who is responsible	When
Organisation of Information Security	Colleagues, Management and Suppliers may not understand the requirements of operating in a secure fashion leaving Post Office systems and data open to accidental or malicious attack, causing data breach or loss of confidentiality, integrity and availability.	A Cyber and Information Security Management System (C&ISMS) must be in place, have senior management approval, be communicated to the entire business and Tested for effectiveness. Please see the Cyber and Information Security Standard, the Supplier Management Standard and the Risk Management Standard	All Staff	Updated Annually

POL00401628

Risk Area	Description of Risk	Minimum Control	Who is responsible	When
Human Resource Security	Poor controls around the selection, on-boarding, termination of staff leads to malicious or accidental data loss, corruption or lack of availability.	Cyber and Information Security Standard. Access Control Standard and the HR Policies	Line Managers	All the time, and evolving with new best practice.
Insider Threat	Poor controls around the usage of Post Office Assets (both logical and physical) by Post Office Staff may impact the Confidentiality, Integrity and Availability of Post Office Data or Impact Post Office reputation by the intentional or accidental misuse of Post Office physical and/or logical Assets.	Acceptable Use Standard	All Staff	All the time, and evolving with new best practice.

POL00401628

Risk Area	Description of Risk	Minimum Control	Who is responsible	When
Asset Management	Poor understanding of the location, flow and destruction of both physical and data assets leads to data loss, corruption or lack of availability	Cyber and information Security Standard, Asset Management Standard and Data Governance Standard. Users of Post Office systems and assets must comply with the Acceptable Use Standard	All Staff	All the time, and evolving with new best practice.
Secure Development of business applications	Poor design of Business applications or lack of consideration regarding security requirements during the design process can lead to the introduction of security vulnerabilities and subsequently result in breaches of data, loss of integrity or data being accessed by unauthorised individuals.	All projects and programmes must liaise with IT Security and the IT Architecture teams for advice and guidance on the security aspects of their designs. All development must comply with the SDLC Standard.	Business Unit CIOs, Project & Programme Managers, and procurement.	At project design phase and during change.

POL00401628

Risk Area	Description of Risk	Minimum Control	Who is responsible	When
Identity and Access Management	Having inappropriate access controls to data owned or processed by Post Office could lead to inappropriate access by unauthorised individuals	All systems must comply with the Access Control Standard. Users of Post Office systems and assets must comply with the Acceptable Use Standard.	Data Owners, Line Managers, Business Unit CIOs, Project and Programme managers, and procurement	Whenever a new system is being designed or procured, or when significant change is being applied.
Security Infrastructure	If the design of systems supporting or running security services for Post Office are not securely designed to the highest standards, those functions cannot be assured and Post Office systems and data may be open to attack, causing data breach or loss of confidentiality, integrity and availability.	All projects and programmes must liaise with IT Security and the IT Architecture teams for advice and guidance on the security aspects of their designs. All infrastructure must comply with the Platform Security Standard, Cloud Computing Standard, Network Security Standard, Cryptography Standard and the Logging and Monitoring Standard where applicable.	Business Unit CIOs, Third party supply chain of IT Services where systems are hosting or processing Post Office Data	All the time, and evolving with new best practice.

POL00401628

Risk Area	Description of Risk	Minimum Control	Who is responsible	When
Network Management	If networks supporting the flow of Post Office information are not designed with security in mind, then those networks themselves may contain vulnerabilities causing a loss of confidentiality, integrity or availability of systems and or data.	All network designs must adhere to the Platform Security Standard, Cloud Computing Standard, Network Security Standard, Physical Security Standard, Code of Connections Standard and the Logging and Monitoring Standard where applicable.	Business Unit CIOs, Third party supply chain of IT Services where systems are hosting or processing Post Office Data	All the time, and evolving with new best practice.
Mobile and removable devices	Poorly controlled mobile and removable devices may lead to a data breach causing a loss of confidentiality, integrity or availability, reputational damage and/or fines from the regulator.	All mobile and removable devices must adhere to the BYOD Standard, Platform Security Standard and the Remote Access and Portable Device Standard where applicable.	All staff	All the time

POL00401628

Risk Area	Description of Risk	Minimum Control	Who is responsible	When
Vulnerability Management	If Post Offices devices (laptops, mobiles, network devices, servers etc.) are poorly configured or maintained and those vulnerabilities are exploited then this could lead to a loss of confidentiality, integrity or availability, reputational damage and/or fines from the regulator	All devices must comply with the Vulnerability Management Standard., the Penetration Testing and Vulnerability Scanning Standard, the Security Infrastructure Standard and the Platform Security Standard.	IT Security and IT Architecture, Third party supply chain of IT Services where systems are hosting or processing Post Office Data	All the time
Cyber Threat Protection	Post Office's environment is compromised due to lack of, or poorly configured cyber threat protection solutions which could lead to a loss of confidentiality, integrity or availability, reputational damage and/or fines from the regulator	All of Post Office's cyber security protection solutions must adhere to the Threat Prevention Standard and incidents must be assessed, reported and resolved using the Incident Management, Breach Reporting standards and the Business Continuity and Recovery standard.	IT Security and IT Architecture, Third party supply chain of IT Services where systems are hosting or processing Post Office Data	All the time

POL00401628

Risk Area	Description of Risk	Minimum Control	Who is responsible	When
Data Governance	Post Office's data or environment is compromised due to the lack of controls required to manage the creation, usage, destruction or archiving of data and documents used for normal Post Office Operations	All Post Office Data should be managed in line with the Data Governance Standard, the Data Classification Handling and Storage standard and the Document and Record Guideline	All staff	All the time, and evolving with new best practice.

POL00401628

3. Where to go for help

Additional Policies

This Policy is one of a set of policies and standards. The full set of policies and standards can be found at:

https://poluk.sharepoint.com/sites/postoffice/Pages/policies.aspx

3.1. How to raise a concern

Any Post Office employee who suspects dishonest or fraudulent activity has a duty to:

- Discuss the matter fully with their Line Manager; or,
- Report their suspicions by telephoning Grapevine on GRO
- If either or both are not available, staff can contact the Post Office's General Counsel, who can be contacted by email at: whistleblowing GRO or by telephone on GRO
- Alternatively staff can use the Speak Up service available on 0800 0484531
- or via a secure on-line web portal: http://www.intouchfeedback.com/postoffice

Post Office encourages members of the public or people not employed by us who suspect [*activity in breach of policy*] to write, in confidence, to the **Chief Executive's Office, Finsbury Dials, 20 Finsbury St, London EC2 9AQ**.

3.2. Who to contact for more information

If you need further information about this standard or wish to report an issue in relation to this standard, please contact Information Protection and Assurance via GRO or IT Security via GRO

12

POL00401628

4. Control

4.1. Policy Version

Date	Version	Updated by	Change Details
12/06/2015	1.0	ISAG	Final QA and release
17/06/2016	1.1	ISAG	Owner details updated to CISO, no further changes after review
20/11/2016	1.2	ISAG	Interim version which was superseded by the new Post Office Operating Model.
26/10/17	1.3	IPA & IT Security	Changed to the new template for policies Changed to reflect the new Post Office structure Minor editorial changes at annual review and a general simplification of the requirements.
31/10/17	1.4	IPA	Updates following Peer review
07/12/18	1.5	IPA	Minor updates on annual review – caused by changes in responsibilities
14/01/20	2.0	IT Security	Updated policy to also inlcude statement to merge Aceeptable Use, IT Security and Document Retention and Dispoal. Approval from RCC

4.2. Document Control

Group Oversight Committee: Risk and Compliance Committee (RCC)
Sign-off Authority: Risk and Compliance Committee (RCC)
Policy Sponsor: Tony Jowett
Policy Owner: Head of IT Security
Policy Author: Hazel Freeman
Approved by: Post Office Ltd RCC

Approved:
Next review: January 2021

12

POL00401628

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)	Amanda Bowe (Chair ARC PO Insurance Director): Item 2
Ken McCall (SID)	Shikha Hornsey (Group CIO): Item 4
Tom Cooper (NED, UKGI)	Rob Wilkins (Portfolio Director): Item 4
Zarin Patel (NED)	Tony Jowett (Chief Information Security Officer): Item 4
	Andrew Goddard (Managing Director, Payzone): Item 5
Regular Attendees:	Mark Dixon (Head of Treasury, Tax & Insurance): Items 6, 7
Tim Parker (Chairman, POL)	Dan Zinner (Chief Transformation Officer): Item 8
Nick Read (CEO)	Sally Smith (MLRO): Item 9
Alisdair Cameron (CFO)	Meredith Sharples (Director, Telecoms): Item 10.4
Ben Foat (General Counsel)	
PWC	
Johann Appel (Head of Internal Audit)	
Mark Baldock (Head of Risk)	
Jonathan Hill (Compliance Director)	
David Parry (Senior Assistant Company Secretary)	

Time		Item	Owner	Action
09:30	1.	Welcome & Conflicts of Interest	Chair	Noting
09:35	2.	Update from Subsidaries:	Amanda Bowe	
		Post Office Management Services (ARC)		Noting
09:40	3.	Previous Meetings	Chair	
		3.1 Minutes: 25 November 2019		Approval
		3.2 Action List		Noting & Input
		3.3 Draft Risk and Compliance Committee Minutes 14 January 2019		Noting
09:45	4.	PCI-DSS and Cyber Security Update	Shikha Hornsey	Discussion
		4.1 PCI-DSS	Rob Wilkins	
		4.2 Cyber Security Update	Tony Jowett	
10:00	5.	Payzone Risk Report	Andrew Goddard	Noting
10:15	6.	Tax Update and Annual Tax Strategy	Mark Dixon	Noting
10:25	7.	Insurance Update	Mark Dixon	Ratify
10:30	8.	Transformation Office Changes	Dan Zinner	Noting

13

Strictly Confidential

POL00401628

POST OFFICE LIMITED

10:40	9.	Money Laundering Reporting Officer (MLRO) Annual Report	Sally Smith	Noting
11:10	10.	Consolidated Report from Risk, Compliance and Internal Audit		
11:10		10.1 Risk Report	Mark Baldock	Noting
11:20		10.2 Compliance Report	Jonathan Hill	Noting
11:30		10.3 Internal Audit Report	Johann Appel	Noting
11.40		10.4 PSD2 Implementation	Meredith Sharples	Noting
11:50		Policies for Approval		Approval
11:55		Any other Business	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

13