POL00247018

Post Office Audit, Risk and Compliance Committee Agenda

Date
30th January 2017

Start Time	Finish Time
14.00 hrs	17.00hrs

Location
Room 1.19 Wakefield

Present	In Attendance		Apologies
• Carla Stent (Chair) • Richard Callard • Tim Franklin • Ken McCall	• Paula Vennells • Al Cameron • Jane MacLeod • Nick Kennett • Alwen Lyons • Paul Hemsley • Mike Morley-Fletcher • Johann Appel • Richard Williams • Amanda Radford • Peter McIver EY	• Owen Woodley (item 3) • Kevin Gilliland (item 3) • Angela Ven Den Bogerd (item3) • Martin Hopcroft (item 3) • Jenny Ellwood (item 3) • Rob Houghton (item 4) • Geoff Smyth (item 4) • Tim Armit (item 8)	

Agenda Item	Action Needed	Purpose	Lead	Time
1. **Welcome and Conflicts of Interest**			Chairman	14.00
2. **Minutes of the meeting held on 17th November 2016, Matters Arising and Actions List**	Approval	To approve the minutes of the meeting held on 17th November 2016, note the Matters Arising and update on the Actions.	Chairman	14.02
3. **Management of Key Operational Risks** • Financial Control update • IT Control update (not for Jan as included in Board paper) • Network Compliance (including EUM update) • Safety • Transformation	Questions & Noting	ARC to note and discuss the top risks highlighted	Al Cameron Owen Woodley/Kevin Gilliland/ Nick Kennett Angela van den Bogerd/ Martin Hopcroft Angela van den Bogerd/ Jenny Ellwood	14.15

POL00247018

Post Office Audit, Risk and Compliance Committee Agenda (cont.)

Agenda Item		Action Needed	Purpose	Lead	Time
4.	**Cyber attack/ Home phone breach**	Questions & noting	ARC to understand the breach; and the consequences and impact on the business and customers	Rob Houghton/ Geoff Smyth/ Nick Kennett	15.00
5.	**Annual Review**			Jane MacLeod	15.20
	• Financial Crime • Legal	Discussion & noting	ARC deep dive on Financial Crime and Legal risks		
6.	**Internal Audit Report**	Questions & noting	ARC to note the Internal Audit Report	Jane MacLeod/ Johann Appel	15.35
7.	**External Audit report**			Peter McIver	15.50
	Update from the External auditors on the External Audit plan	Noting	Verbal update on the External Audit plan from the External Auditor		
8	**Risk Update**	Questions & noting		Mike Morley-Fletcher	16.10
	Risk report overview, including:				
	• Highlighting the top risk of the Business via the Group Risk Profile		The ARC to note changes to key risks and "Risks of the Moment"		
	• incidents and exceptions,		The ARC to note any incidents/ exceptions since the last meeting.		
	• Risk Appetite		The ARC to feedback on approach to Risk Appetite.		
	• Business Continuity Planning		To update the ARC on BCP.	Jane MacLeod/ Tim Armit	
9.	**Noting papers** • Horizon Scanning	Noting	To update the Arc on new developments	Jane MacLeod	16.30
10.	**Any Other Business**		Topics raised under Any Other Business	Chairman	16.35
11.	**ARC session [with the risk team]**			Chairman/ Jane MacLeod	16.40
	CLOSE				17.00

POL00247018

Appendix to Action 1642(i) EUM Update to ARC

Enhanced User Management Update to ARC – January 2017

The EUM project is making good progress across the core streams of funding, solution build/implementation and audit:

Funding

- The EUM Delivery programme budget has been ratified by POL ESG, with a recommendation going to the POL Board in January 2017 to approve the £7.8m investment. This encompasses EUM build and delivery execution across the wider branch network.

Solution build and implementation

- A working prototype of the EUM core software (that regulates user access to transaction processing systems) is available and key functionality has been demonstrated to stimulate final shaping of the system minimal viable product (MVP). MVP product build and user acceptance testing, which are being achieved using an agile approach, will be completed by February 2017.
- In parallel, activity is underway to execute data cleansing (of vetting and training data from legacy repositories) and to design the integration with Success Factors for user vetting and training/competency management
- The programme is on schedule to commence a 25 branch pilot in March 2017 with full network rollout occurring in July 2017.
- Full network rollout of EUM capability is still to be planned, but is expected to be completed by November 2017.

Audit

- POL Legal has completed a review of the top 20 POL contracts (including those associated with the Banking Framework, POMS and for Bank of Ireland) to ensure that all obligations relating to vetting/training (principally compliance and audit orientated) will be satisfied by the future EUM system and enhanced business processes. The conclusion is that EUM as defined will addresses obligations for these contracts.
- A 50 branch desk audit across a sample of directly managed and agency branches has been completed by POL Internal Audit to assess the efficacy of existing record keeping for vetting and training records. While the work is scheduled to deliver in January, early findings confirm that existing data capture and record retrieval processes for agency branches (the key concern for POMS and Banking Framework) are operating satisfactorily.

Conclusion:

- The project is making good progress and is on track to deliver a robust, long term solution for Post Office.
- The positive audit results in agency branches, combined with the wider project status and other actions being undertaken by POMS, should enable POMS management to recommend to the POMS board at its January meeting that, while the sales processes remains outside appetite, there is an evident route to achieving appetite within a reasonable timeframe; as such I would have confidence that the POMS board would support the continued sale of travel insurance in agency branches while the project is fully implemented; following the rollout of a new protection model in January, life assurance sales will be restricted to a limited number of branches, thereby significantly limiting the risks associated with this product).

POL00247018

Strictly Confidential

Post Office Limited ARC Committee

Status Report as at: 23 January 2017

Action included on the ARC agenda
Action closed

REFERENCE	ACTION	Action Owner (GE Member)	Due Date	STATUS	Open/Closed
22 January 2016 POLARC 16/03 (q)	Risk Update For the Executive to work with the external auditors to set out what a three year roadmap to benchmark against the UK Corporate Governance Code would like.	**General Counsel**	**September 2017** ARC	Corporate Governance Capability - The Chairman of the ARC & GC have agreed to revisit the benchmarking with the UK Corporate Governance Code in a years time September 2017 ARC	Open
19 May 2016 POLARC 16/27 (i)	Risk and Control Update To carry out a further BCP test in due course and include the test in the Horizon report to the ARC in September.	**General Counsel**	**January 2017** ARC	Was due on September and November ARC agendas but owing to resourcing issues (which have now been resolved) will be reported to January ARC. BCPP Manager will report on the work done to date, the adequacy of the Post Office's current BCP planning and implementation, together with further planned remediation activity in 2017.	Closed
28 September 2016 POLARC 16/42 (i)	POMS as Principal: Implementation of Horizon (IT) User Access Control The ARC stressed the importance of implementing the new control to manage user access and the Chair asked the CEO to provide a report setting out the timeline and actions to deliver the requirement.	**Nick Kennett**	**January 2017** ARC	A project team has been stood up to design, build and implement End User Management (EUM) the Horizon User Access Control. Good progress is being made across all work streams. An update appended to these actions is provided for January ARC. The update provides the latest status and key actions on the project.	Closed
28 September 2016 POLARC 16/43 (d)	BOI UK Report GG suggested that the Capability Development Managers provided by BoI could be better used to help POL and OW agreed to work with BoI to determine what would be possible in this regard.	**Owen Woodley**	**November 2016** ARC	BOI are working on a change of structure for the CDM community and once this is completed, we have agreed to establish joint governance to measure the value of their activity and refocus their attention on a regular basis in areas of highest benefit. This governance has not occurred before and will enable us to be much more proactive in the use of this resource.	Closed
28 September 2016 POLARC 16/43 (e)	BOI UK Report JH to provide the Post Office Money Conduct Risk Dashboard to the ARC on a quarterly basis.	**Jonathan Hill**	**January, March, September and November 2017 ARC**	This is ongoing and to be added to the POL ARC agenda quarterly. Dashboard included with ARC papers.	Closed
28 September 2016 POLARC 16/43 (g)	BOI UK Report A review of the 2nd and 3rd lines of defence in the Post Office Money branch distribution model to be undertaken in autumn 2017/18.	**General Counsel**	**September 2017 ARC**		Open
28 September 2016 POLARC 16/44 (d)	POL Financial Services The ARC asked POMS to consider developing a similar dashboard to that produced by BoI to facilitate POL's reporting to the ARC on the KPIs POL should monitor in regard to its role as AR to POMS. Ideally this reporting would be quarterly.	**Nick Kennett**	**January 2017** ARC	NK has provided a preliminary dashboard from POMS on its assessment of customer conduct management including POL's role as AR - it is draft and will be updated through 2017 to make data more "visible" and as changes to the upstream suppliers allow easier access to data.	Closed

POL00247018

REFERENCE	ACTION	Action Owner (GE Member)	Due Date	STATUS	Open/Closed
17 November 2016 POLARC 16/57 (c)	Risk Report Overview - Risk Appetite Statements The Committee asked MMF to ensure that the work focussed on producing clear risk appetite statements which could be used to highlight exceptions, rather than focus on collating and reporting too many metrics.	**Mike Morley Fletcher**	**January 2017 ARC**	Included in January ARC agenda.	Closed
17 November 2016 POLARC 16/57 (d)	Risk Report Overview - Financial Crime and Fraud Risk Deep Dive Financial Crime and Fraud risk would be tabled at the January meeting as a deep dive.	**Mike Morley Fletcher**	**January 2017 ARC**	Included in January ARC agenda.	Closed
17 November 2016 POLARC 16/57 (e)	Risk Report Overview - Simple Summary Tracker for Risk Exceptions A simple summary tracker to report risk exceptions would be presented to future Committees, starting in January. The CEO asked that the extent of detail required in the approval form for a risk exception should be reviewed and simplified.	**Mike Morley Fletcher**	**January 2017 ARC**	Included in January ARC agenda.	Closed
17 November 2016 POLARC 16/59 (g)	Transformation Risk Update - Reporting of Transformation Portfolio Risks DH agreed that in future the report would provide a narrative on the top red risks; a tracker of the risk movement; and the portfolio risks as shown in the table on page 7 of the report. DH would design a shorter report and agree the content with the Chair ready for production for the next ARC.	**David Hussey**	**January 2017 ARC**	Included in January ARC agenda.	Closed
17 November 2016 POLARC 16/60 (c)	Perimeter Controls - IT Controls Plan The CIO would report on the progress (of IT controls) at the January ARC. The ARC asked that business impact to be made clear in the reporting and where possible a link to operational metrics and the strategy.	**Rob Houghton (CIO)**	**January 2017 ARC**	Report to January Board	Closed
17 November 2016 POLARC 16/66 (e)	EY Plan for 2016/17 Audit Including New Team - FRES The materiality level for FRES would be aligned to that of POL and similar to last year. PMI to send PwC the relevant instructions for FRES.	**Peter McIver (EY)**	November 2016	Peter McIver to update Committee at the January meeting.	Open
17 November 2016 POLARC 16/67 (e)	Network Conduct Risk Action Plan - Quarterly Updates The Committee asked for a quarterly update on the network control risks that were causing most concern and an assessment of progress to mitigate these risks.	**Kevin Gilliland**	**January 2017 ARC**	Included in ARC papers.	Closed
17 November 2016 POLARC 16/72 (b)	Internal Audit Report - IT Disaster Recovery and Resilience The committee asked for an update on the IT Disaster Recovery and Resilience, which would be covered in the January Board review of IT.	**Rob Houghton (CIO)**	**January 2017 ARC**	Report to January Board	Closed

POL00247018

Appendix to Action POLARC 16/44(d)

CONDUCT RISK SCORECARD

			Rating Criteria			Current					
Conduct Outcome	**Area**	**Measure**	**Green**	**Amber**	**Red**	**Oct**	**April**	**May**	**June**	**July**	**Aug**
We strive to ensure that customers receive a high quality service when they deal with us or where things go wrong	Complaints	Number of Opened complaints	0-1,000	1,000 - 1,500	1,500 - 2,000	391	888	786	687	645	554
		Percentage of upheld complaints	0% - 20%	21% - 30%	31% - 100%	29.0%	25.9%	25.7%	24.3%	28.2%	28.9%
		% of complaints to PIF for the month	0% - 0.2%	0.2% - 0.5%	0.5%+	0.05%	0.12%	0.10%	0.09%	0.09%	0.07%
		No of FOS referrals upheld	0 - 3	4 - 7	8 +	2	0	2	2	2	1
Treating Customers Fairly is central to the behaviour of our staff in product, sales and post sales roles	Mystery Shopping	Proportion of shops rated red in the month	0% - 10%	11% - 20%	20% - 100%	0%	7%	33%	19%	0%	20%
		Number of shops rated black in month	0	0	1	0	0	0	0	0	0
	Call Validation	[Not sure how this is measured]									
	Call Monitoring (Travel)	Percentage of red rating calls in the month	0% - 5%	6% - 10%	10% - 100%	6%	8%	6%	5%	5%	5%
We design and price our products to deliver value for our customers and to perform as expected	Cancellations (Motor, Business, Pet)	Percentage of products to sales, cancelled within the cooling off period (14 days)	0 % - 5%	6% - 10%	11% - 100%	3.4%	2.7%	2.7%	2.9%	2.5%	2.7%
	Cancellations (Life & Over 50s)	Percentage of products to sales, cancelled within the cooling off period (30 days)	0 % - 5%	6% - 10%	11% - 100%	4.3%	4.3%	3.7%	6.5%	5.0%	6.7%
	MTCs	Percentage of products to PIF, cancelled after the cooling off period	1 % - 10 %	11% - 20%	21% - 100%	8.1%	6.7%	7.0%	7.0%	7.4%	7.7%
	Claims (Travel, Protection and Pet)	Percentage of claims repudiated	0% - 5%	6% - 10%	11% - 100%	9.3%	12.3%	11.2%	12.3%	8.6%	7.4%
We train our staff to provide informative customer service and post sales experience	Training & Competence	Percentage of POMS staff completed mandatory training	100% - 95%	95% - 90%	90% - 0%						
		Percentage of Call Center staff completed mandatory training	100% - 95%	95% - 90%	90% - 0%	100%	100%	100%	100%	100%	100%
		Percentage of Branch staff completed mandatory training	100% - 95%	95% - 90%	90% - 0%						
		Financial Specialists signed off as competent	100% - 90%	90% - 80%	80% - 0%	95%	89%	88%	90%	88%	92%
		Number of Specialists not observed for product knowledge within 3 months	0-5	06-Oct	11+	0	4	5	1	8	4
		Number of Specialists suspended	0 - 5	6 - 10	11+	11	5	8	9	6	5
We organise ourselves in an appropriate and controlled manner with customer satisfaction central to our ethos	Customer Satisfaction (CES)	Proportion of customer responses to NPS surveys that confirm adequate information was provided at the point of sale in the previous 3 months				95%	92%	94%	93%	95%	92%
	Net Promoter Score (NPS)		35	34-30	>30	43	42	51	43	39	42
We market and sell our products through all our channels in the most appropriate way to ensure customers understanding and	Financial Promotions	Financial Promotion Breaches recorded in the previous 3 months	0-5	6-10	11+	0	0	0	0	0	0
		Financial Promotions expired in the period	0-20	21-40	41+	0	6	43	9	38	39
We manage a robust framework of Risk Management including the assessment, control and monitoring of conduct risk	Incidents	Number of Severe Incidents (rated 1 or 2)	0	1	2	1	2	0	0	1	0
		New Incidents in the period	0-4	5-9	10+	4	5	3	2	3	1
		Number of Open Incidents	0 - 10	10 - 20	20+	10	21	18	20	14	11

POL00247018

Appendix to Action POLARC 16/43(e)

Post Office Money branch distribution

How we performed against our aims in December 2016

Using a range of key risk indicators, we measure our conduct performance against each of our FACE Customer Charter commitments and promises. This tells us how well we're doing against our targets and highlights areas where we could improve our performance. We also use our performance to give ourselves an overall risk rating. This month, we rated our overall performance as Amber. The risk ring shows the relative ratio of green, amber and red rated key risk indicators. Our tolerances are shown on page 13.

Our risk ratings

Our November risk ratings and how they compare to October

Red rated mystery shops	◄►
Black rated mystery shops	▲
Mutiple red/black shops	◄►
A or B rated mortgage cases	◄►
D rated mortgage cases	◄►
MS meeting QAT benchmark	▼
Distribution complaints	◄►
Advice/information complaints	◄►
Conduct survey results	◄►
NPS survey results	◄►
Branch product knowledge	◄►
Branch regulatory knowledge	◄►
Specialist/CRM knowledge	◄►
Branch advertising reviews	◄►
Advertising breaches/issues	▼
Social media breaches/issues	◄►
Savings cancellations	◄►
Matched credit card usage	◄►
Competent specialists	◄►
Supervisor spans of control	◄►
BOI supervisor reviews	◄►

Our performance

How we performed against our FACE Customer Charter commitments and promises in November

Risk ring and overall performance rating



Based on the weighted cumulative outcome of the KRIs we measured this month, our overall risk rating for November is Amber.



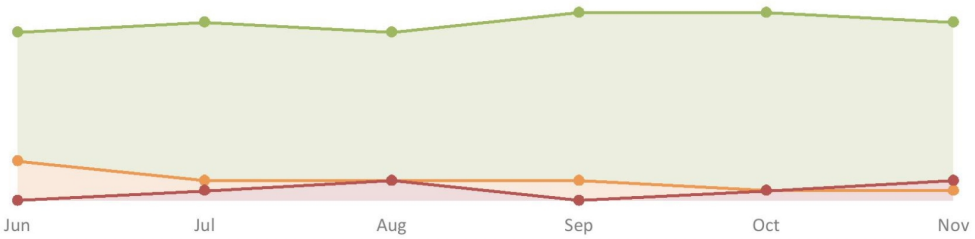
This month we were within tolerance for 19 out of the 21 KRIs we measured. 18 of our KRIs were rated green and one of our KRIs was rated amber. 2 of our KRIs were rated red. In comparison, in October we exceeded tolerance in one of our KRIs and in September we were within tolerance in all our KRIs. On average, in each month between June and November, we were within tolerance in 20 of the KRIs we measured and exceeded tolerance in only one.

November ratings v October ratings

◄►	17
◄►	1
◄►	0
▲	1
▲▼	0
▼	2

Red KRIs - one KRI moved out of red and 2 KRIs fell to red.

Distribution of KRI risk ratings between June 2016 and November 2016



Exceptions and key trends

Mortgage Specialist mystery shops - Overall levels of red rated shops for Specialists fell again to 5.9% for the three months ending in November. The proportion of red-rated Mortgage related shops rose slightly to 22%, however, this was based on a small sample size, with 2 out of 9 shops being rated red in the three months ending in November, and one out of three being rated red in November. No shops were rated 'black' in November. Post Office are taking steps designed to ensure that Mortgage Specialists maintain competence in periods of low productivity, and an action plan in this regard was agreed with the Customer and Conduct Risk Committee In November. The impact of this will be monitored over the next 3-4 months.

Mortgage Specialist QAT checks - Five of the 31 Mortgage Specialists who had cases checked in November fell below the QAT benchmark, with less than 80% of their cases being rated A or B. However, this figure is significantly distorted by the low number of cases submitted. Of the five Specialists falling below the benchmark, four submitted only one case in the month and the other submitted only two cases.

Financial promotions breaches - three material breaches were recorded by the BOI Financial Promotions Team in November. The FCA contacted the Bank expressing concerns in relation to the online promotion of the interest free period on the Post Office Balance Transfer Credit Card. In particular, the FCA questioned the prominence of the warning that any interest free period would be for 'up to' 37 months. Following discussions with Post Office, the material was amended accordingly. In addition, live versions of online affiliate material relating to Mortgages and Credit Cards were found to differ from the approved versions. The material has been corrected and the underlying causes are being investigated.

◄► Remained green ◄► Remained amber ◄► Remained red ▲ Improved to green ▲ Improved to amber ▼ Fell to amber ▼ Fell to red

POL00247018

Appendix to Action POLARC 16/43(e)

How we performed against our FACE Customer Charter

Our FACE Customer Charter sets out a range of commitments and promises designesd to put customers at the heart of our business. Our aims describe how we will meet each of these commitments and promises and using a range of key risk indicators, we set ourselves targets and tolerances, and measure our performance against these. We rate our performance either green or amber if we are within tolerance, or red if we are outside of tolerance. This tells us how well we're doing against our targets and highlights areas where we could improve our performance.

Our customer charter	Our aims	Our performance			
Our commitments and promises	**How we meet our commitments and promises**	**We use a range of key risk indicators to measure our performance against our aims and to highlight areas where we need to improve**			
		How we measure ourselves	Our targets and tolerances	How we're doing Nov-16	Oct-16
Fair - you are at the heart of everything we do	We provide information and advice that our customers can rely on	We use **mystery shoppers** to test how well our staff are meeting our conduct risk requirements and our customer's needs	Fewer than 20% of mystery shops are rated red in the quarter	5.9%	8.6% ▲
			No shops are rated black in the month	0	1 ▲
			Fewer than 10% of our Specialists have more than one red or black shop in the preceeding six months	2.0%	1.0% ▲
		Our Quality Assurance Team assess the **quality of the mortgage advice** we give customers to ensure it's suitable to their needs	At least 80% of cases are rated A or B by the QAT in the month	92%	100% ▼
			Fewer than 6% of cases are rated D by the QAT in the month	3.2%	0.0% ▼
			At least 85% of MSs meet the QAT benchmark in the month	85%	97% ▼
		We use branch reviews and monitor breaches to ensure our **financial promotions** are compliant and up to date, and our social media use is compliant	90% or more of our branch reviews are rated green or amber for financial promotions in the quarter	98%	97% ▲
			We record fewer than 4 material breaches and no systemic conduct issues in relation to financial promotions	4	1 ▼
			We record fewer than 7 material breaches and no systemic conduct issues in relation to social media	3	3 ◀▶
	We do our best to get things right first time and act quickly to put it right if we don't	We monitor **customer complaints** to understand what we're getting wrong and why, and to ensure we get it right in the future	We uphold fewer than 1 distribution complaint for every 100 products we sell	0.73	0.65 ▼
			We uphold fewer than 0.26 advice or information complaints for every 100 products we sell	0.03	0.15 ▲
Accessible - we provide a friendly, efficient and reliable service	We listen to our customers and act when they tell us we could do things better	We use **customer feedback** to tell us whether we met their needs at the point-of-sale	At least 90% of compliance survey questions confirm customer's needs and compliance standards are met in the quarter	98.8%	98.2% ▲
			At least 90% of NPS surveys confirm customers receive the information they need in the quarter	95.6%	97.0% ▼
Committed - we aim to build long-term relationships	We have staff with the requisit levels of skill, knowledge and expetise	We use the results of **knowledge tests** to ensure our staff have the skills, knowledge and expertise to meet our customer's needs	At least 80% of BOI product knowledge reviews are rated green or amber in the quarter	100%	100% ◀▶
			At least 80% of BOI regulatory awareness reviews are rated green or amber in the quarter	95%	97% ▼
			Specialists pass at least 80% of POL knowledge tests in the quarter	99.7%	99.2% ▲
		We monitor our **training and competence** arrangements to ensure staff are maintaining their competence and are being adequately supervised	At least 80% of Specialists are signed off as fully competent	92.6%	94.6% ▼
			At least 80% of FSAMs are within agreed spans of control	96%	96% ◀▶
			At least 80% of BOI FSAM reviews are rated green or amber in the quarter	100%	100% ◀▶
Easy to do business with - we promise to keep it simple and straightforward for you	Our products are easy to understand and meet customer's needs and expectations	We monitor the **retention and use of our products** by customers to ensure they meet their needs and expectations	Customers cancel no more than 1.5% of savings products in the cooling-off period	0.49%	0.86% ▲
			At least 80% of Matched credit cards sold in-branch are subsequently used by customerss	89%	90% ▼

▲ Performance improving from previous month ▼ Performance worsening from previous month ◀▶ Performance unchanged from previous month

BOI Group classification : **Red** (confidential)

POL00247018

Appendix to Action POLARC 16/43(e)

Current performance and recent trends

Our key risk indicators	Our performance		
How we measure ourselves	How we did in November	Compared to October	Over each of the last six months (Jun 16 to Nov 16)
The proportion of mystery shops rated red in the last three months	5.9%	▲ -2.7%	12.2% 10.8% 12.5% 11.3% 8.6% 5.9%
The number of mystery shops rated black in the last month	0	▲ -1	0 0 1 0 1 0
The proportion of Specialists with multiple red or black mystery shops in the last six months	2.0%	▲ 1.0%	0.8% 0.9% 1.9% 1.0% 1.0% 2.0%
The proportion of mortgage cases checks rated A or B in the last month	92%	▼ -8%	91% 93% 97% 94% 100% 92%
The proportion of mortgage cases checks rated D in the last month	3.2%	▼ +3.2%	2.3% 1.1% 1.7% 3.8% 0.0% 3.2%
The proportion of Specialists with over 80% of their mortgage case checks rated A or B	84.8%	▼ -12.1%	86.2% 90.7% 93.9% 93.1% 97.0% 84.8%
The number of branch distribution complaints upheld for every 100 branch sales	0.73	▼ +0.08	0.86 1.34 1.16 0.57 0.65 0.73
The number of branch advice or information complaints upheld for every 100 branch sales	0.03	▲ -0.12	0.13 0.20 0.17 0.11 0.15 0.03
The results of conduct surveys	99%	▲ +0.5%	96% 97% 96% 97% 98% 99%
The results of NPS surveys	96%	▼ -1.4%	97% 99% 99% 98% 97% 96%
The results of BOI branch product knowledge reviews	100%	◀▶ 0.0%	100% 100% 100% 100% 100% 100%
The results of BOI branch regulatory knowledge reviews	95%	▼ -2.1%	100% 100% 100% 97% 97% 95%
The results of POL Specialist knowledge tests	100%	▲ +0.5%	99.2% 99.2% 99.2% 99.2% 99.2% 99.7%
The results of BOI branch financial promotions reviews	98%	▲ +0.4%	100.0% 96.9% 97.1% 93.3% 97.1% 97.5%
Material breaches and systemic conduct issues in relation to financial promotions	4	▼ +3	1 0 0 0 1 4
Material breaches and systemic conduct issues in relation to social media use	3	◀▶ -	0 0 0 0 3 3
Savings products cancelled by customers	0.5%	▲ -0.4%	0.75% 0.76% 0.67% 0.75% 0.86% 0.49%
Matched credit cards used by customers	89%	▼ -1.6%	89.9% 92.1% 91.2% 91.0% 90.3% 88.7%
Specialists signed-off as fully competent	93%	▼ -2.0%	88% 87% 91% 93% 95% 93%
FSAMs within agreed supervisory spans of control	96%	◀▶ 0.0%	100% 96% 96% 96% 96% 96%
BOI FSAM supervisory reviews rated green or amber	100%	◀▶ 0.0%	100% 96% 95% 95% 100% 100%

Performance ratings: ▲ Performance improving ▼ Performance worsening ◀▶ Performance unchanged

BOI Group classification : **Red** (confidential)

POL00247018

Appendix to Action POLARC 16/43(e)

Trends and exceptions

Mystery shopping

Specialists - Levels of red rated shops fell again to 5.9% for the three months ending in November. The proportion of red-rated Mortgage related shops rose slightly to 22%, however, this was based on a small sample size, with 2 out of 9 shops being rated red in the three months ending in November, and one out of three being rated red in November. No shops were rated 'black' in November. Post Office are taking steps designed to ensure that Mortgage Specialists maintain competence in periods of low productivity, and an action plan in this regard was agreed with the Customer and Conduct Risk Committee In November. The impact of this will be monitored over the next 3-4 months. (Action 012)

CRMs - Red rated savings mystery shops for CRMs fell again to 8% for the three months to the end of November, with no shops being rated red in October or November.

Knowledge and awareness

One Directly Managed branch - Haywards Heath - was rated red in relation to regulatory knowledge by the BOI Risk Assurance Team in November. The exceptions noted related to staff knowledge in relation to a complainant's right of FOS referral, the mandatory completior of the POL Regulatory Workbook, staff knowledge of the sales process - in particular, in relation to product comparisons and the provision of financial advice - and staff being unable to locate operational branch procedures. These findings were fedback to the Branch Manager, who was directed to take action to improve the knowledge of staff in these areas.

No other material exceptions or hot spots were identified.

Quality of mortgage advice

The overall pass rate fell from 100% in October to 92% in November, although this is still well above the tolerance of 80%. 64% of cases were rated A, which is above the target level of 60% for the second month in a row.

Five of the 31 Mortgage Specialists who had cases checked in November fell below the QAT benchmark, with less than 80% of their cases being rated A or B. However, this figure is significantly distorted by the low number of cases submitted. Of the five Specialists falling below the benchmark, four submitted only one case in the month and the other submitted only two cases. As such, it is recommended that the metric be amended to take account of cases submitted over either a rolling three or six month period. This recommendation will be presented to the C&CRC in December.

Financial promotions and social media

Three material breaches were recorded by the BOI Financial Promotions Team in November:
(1) Balance transfer credit card online material - the FCA contacted the Bank expressing concerns in relation to the promotion of the interest free period on the Post Office Balance Transfer Card. In particular, the FCA questioned the prominence of the warning that any interest free period would be for 'up to' 37 months. Following discussions with Post Office, the material was amended accordingly.
(2) Mortgage 'pay per click' online material - The live version of the material differed to that approved, as a result of errors by the agency. The material was subsequently corrected.
(3) Credit card affiliate online template - The live version of the material differed to that approved. The material has been corrected and the underlying cause of this issue is still under investigation.

No social media breaches were reported by Post Office in November.

Customer complaints

Levels of upheld branch distribution and 'advice and information' related complaints increased very slightly, but remained within tolerance in November.

28 branch distribution complaints were upheld in November, compared to 27 in October. 17 of these related to savings, 7 related to current account and 4 related to credit card. Of these 28 complaints, only one related to advice or information.

Product retention and usage

Savings cancellations - No 'hot spots' or issues identified.

Credit card usage - This KRI has now been updated to reflect the three month usage level of the Matched card only and is rated green. Although still amber rated, usage rates for the Platinum card have slowly improved over the last six months, rising to 74% for November. The C&CRC acknowledges that the Platinum card is primarily designed and promoted for holiday use and that the other management information and KRIs in this regard are not suggestive of systemic branch mis-selling.

Customer insight

No 'hot spots' or issues identified.

Training and competence

Although within tolerance, the proportion of Mortgage Specialists yet to be signed off as 'fully competent' remains amber rated at 83.5% (66 out of 79). This situation continues to be actively monitored and managed by POL FS Risk T&D, with low levels of sales activity or temporary withdrawal due to non-competence continuing to result in delays in signing individuals off as fully competent. In addition, five new Mortgage Specialists are now under close/enhanced supervision.

POL00247018

Appendix to Action POLARC 16/43(e)

Mystery shopping

We use mystery shoppers to test how well our staff are meeting our conduct risk requirements and our customer's needs

Our targets	Our performance		
The minimum standards we expect to achieve	**How we did in November**	**Compared to October**	**Over each of the last six months (June 2016 to November 2016)**
Red shops - Fewer than 20% of mystery shops are rated red in the quarter	5.9%	▲ -2.7%	12.2% 10.8% 12.5% 11.3% 8.6% 5.9%
Black shops - No mystery shops are rated black in the last month	0	▲ -1	0 0 1 0 1 0
Multiple fails - Fewer than 10% of our Specialists have multiple red or black shops in the last six months	2.0%	▲ 1.0%	0.8% 0.9% 1.9% 1.0% 1.0% 2.0%

Trends and exceptions

Specialists - Levels of red rated shops fell again to 5.9% for the three months ending in November. The proportion of red-rated Mortgage related shops rose slightly to 22%, however, this was based on a small sample size, with 2 out of 9 shops being rated red in the three months ending in November, and one out of three being rated red in November. No shops were rated 'black' in November. Post Office are taking steps designed to ensure that Mortgage Specialists maintain competence in periods of low productivity, and an action plan in this regard was agreed with the Customer and Conduct Risk Committee In November. The impact of this will be monitored over the next 3-4 months. (Action 012)

CRMs - Red rated savings mystery shops for CRMs fell again to 8% for the three months to the end of November, with no shops being rated red in October or November.

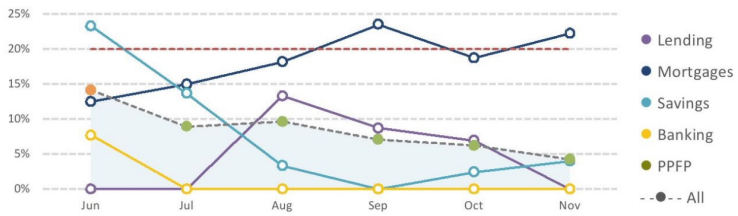
All red rated mystery shops (rolling 3 months)

136 mystery shops were completed between September and November. 91.2% (88.2%) were rated green or amber and 5.9% (8.6%) were rated red. There were no black rated shops in November , 1 less than in October. In the last six months there have been 2 black shops.



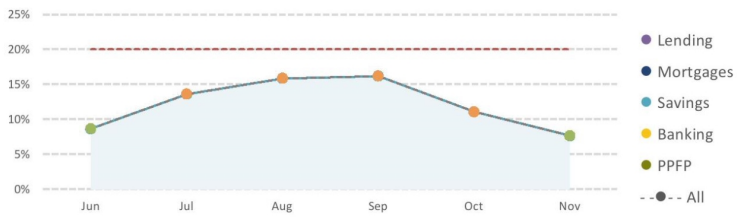
Crown Specialist - red shops (rolling 3 months)

The risk rating for Crown Specialist shops is currently green. 71 of the shops between September and November related to Crown Specialists, of which 3, or 4.2% (6.2%), were rated red. One of the 14 Specialist shops completed in November - 7.1% - was rated red. At the end of November, 4 specialists had received multiple red or black shops in the preceding six months.



Agency Customer Relationship Manager - red shops (rolling 3 months)

The risk rating for Agency CRM shops is currently green. 65 of the shops completed between September and November related to Agency CRMs, of which 8% (11.1%) were rated red. No CRM shops were rated red in November.



Last month's performance shown in brackets

POL00247018

Appendix to Action POLARC 16/43(e)

Quality of mortgage advice

Our QA Team assess the quality of the mortgage advice we give customers to ensure it's suitable to their needs

Our targets	Our performance		
The minimum standards we expect to achieve	How we did in November	Compared to October	Over each of the last six months (June 2016 to November 2016)
A/B rated cases - At least 80% of cases are rated A or B by the QAT in the month	92.1%	▼ -7.9%	90.6% 93.1% 96.6% 94.3% 100.0% 92.1%
D rated cases - fewer than 6% of cases are rated D by the QAT in the month	3.2%	▼ +3.2%	2.3% 1.1% 1.7% 3.8% 0.0% 3.2%
MS meeting benchmark - At least 85% of MSs meet the QAT benchmark in the month	84.8%	▼ -12.1%	86.2% 90.7% 93.9% 93.1% 97.0% 84.8%

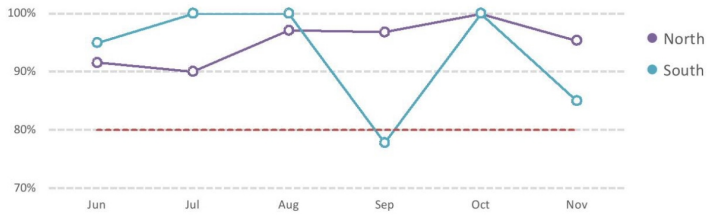
Trends and exceptions

The overall pass rate fell from 100% in October to 92% in November, although this is still well above the tolerance of 80%. 64% of cases were rated A, which is above the target level of 60% for the second month in a row.

Five of the 31 Mortgage Specialists who had cases checked in November fell below the QAT benchmark, with less than 80% of their cases being rated A or B. However, this figure is significantly distorted by the low number of cases submitted. Of the five Specialists falling below the benchmark, four submitted only one case in the month and the other submitted only two cases. As such, it is recommended that the metric be amended to take account of cases submitted over either a rolling three or six month period. This recommendation will be presented to the C&CRC in December.

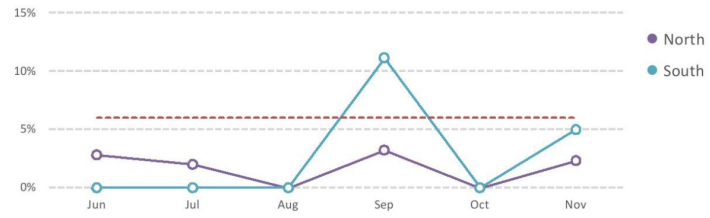
Mortgage cases rated A or B by QAT (monthly)

The Quality Assurance Team (QAT) performed 63 mortgage case checks in November. 92% (100%) of cases passed the initial review. 41 out of 43 cases submitted by the northern region were rated A or B and 17 out of 20 cases submitted by the southern region were rated A or B.



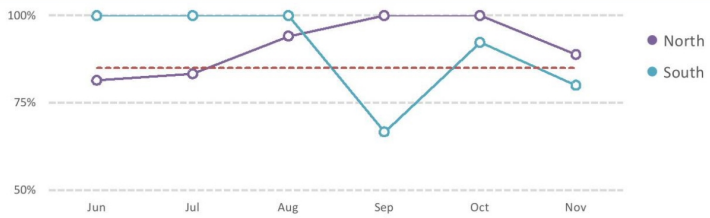
Mortgage cases rated D by QAT (monthly)

3% of cases were rated 'D' in November, compared to 0% in October. There was one 'D' rated case in the northern region and one 'D' rated case in the southern region.



Specialists meeting QAT benchmark (monthly)

85% (97%) of Specialists met the QAT benchmark this month, with at least 80% of their cases passing the initial QAT check. 5 (1) Specialists did not.



Last month's performance shown in brackets

POL00247018

Appendix to Action POLARC 16/43(e)

Customer complaints

We monitor complaints to understand what we're getting wrong and why, and to ensure we get it right in the future

Our targets	Our performance		
The minimum standards we expect to achieve	**How we did in November**	**Compared to October**	**Over each of the last six months (June 2016 to November 2016)**
Distribution complaints - Fewer than 1 complaint is upheld for every 100 sales	0.73	▼ +0.08	0.86 1.34 1.16 0.57 0.65 0.73
Advice/information complaints - Fewer than 0.26 complaints are upheld for every 100 sales	0.03	▲ -0.12	0.13 0.20 0.17 0.11 0.15 0.03

Trends and exceptions

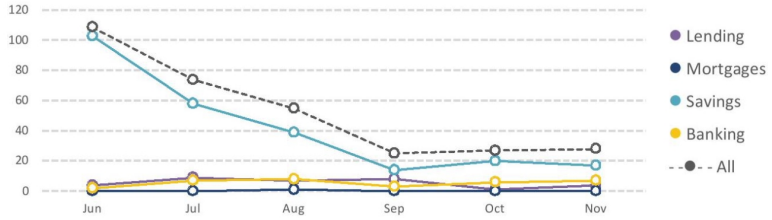
Levels of upheld branch distribution and 'advice and information' related complaints increased very slightly, but remained within tolerance in November.

28 branch distribution complaints were upheld in November, compared to 27 in October. 17 of these related to savings, 7 related to current account and 4 related to credit card. Of these 28 complaints, only one related to advice or information.

Upheld branch distribution complaints (monthly)

Overall, compared to last month, the number of branch distribution complaints upheld increase by 1, from 27 to 28.

Lending complaints increase by 3 to 4, mortgage complaints remained the same, savings complaints decreased by 3 to 17 and banking complaints increase by 1 to 7.



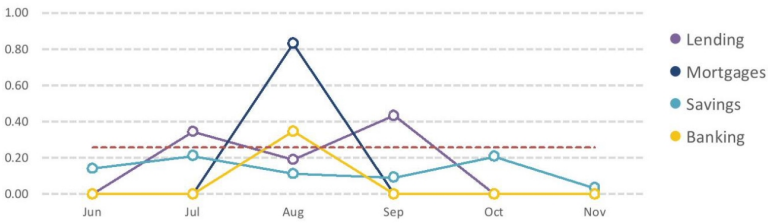
Upheld branch distribution complaints for every 100 sales made (monthly)

28 branch distribution complaints were upheld in November, 1 more than in October. This means that 0.73 branch distribution complaints were upheld for every 100 in-branch sales made. Putting it another way, there was one upheld branch distribution complaint for every 137 sales made.



Upheld branch advice or information complaints for every 100 sales made (monthly)

One advice or information complaint was upheld in November, 5 less than in October. This means that 0.03 advice or information complaints were upheld for every 100 in-branch sales made. Putting it another way, there was one upheld advice or information complaint for every 3,830 sales made.



POL00247018

Appendix to Action POLARC 16/43(e)

Customer insight

We use customer feedback to tell us whether we met their needs at the point-of-sale

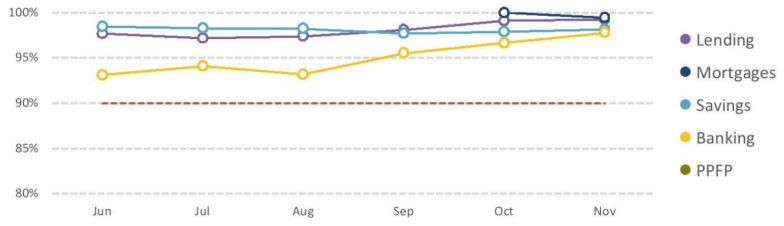
Our targets	Our performance		
The minimum standards we expect to achieve	**How we did in November**	**Compared to October**	**Over each of the last six months (June 2016 to November 2016)**
Conduct surveys - At least 90% of conduct survey questions demonstrate compliance	98.8%	▲ +0.5%	96.4% 96.5% 96.3% 97.1% 98.2% 98.8%
NPS surveys - At least 90% of NPS surveys confirm customers receive the information they need	95.6%	▼ -1.4%	97.4% 98.8% 98.7% 97.7% 97.0% 95.6%

Trends and exceptions

No 'hot spots' or issues identified.

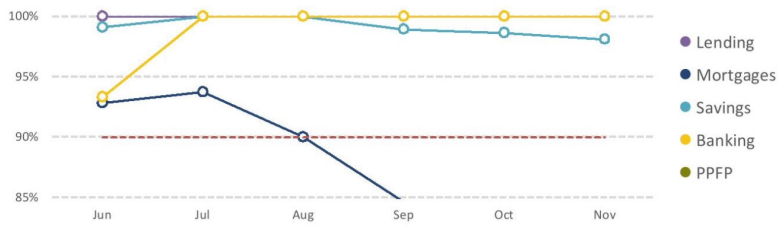
Conduct survey results (rolling 3 months)

192 conduct surveys were completed in the three months to the end of November. 99% of responses indicated conduct-related point-of-sale requirements were met and no product areas were rated red.



NPS survey results (rolling 3 months)

68 NPS surveys, where customers gave 'non-passive' responses when asked to rate the information they received from a Specialist, were completed in the three months to the end of November. 96% of these responses confirmed customers were satisfied with the information they received from the Specialist and no product areas were rated red.



POL00247018

Appendix to Action POLARC 16/43(e)

Knowledge and awareness

We use knowledge tests to ensure our staff have the skills, knowledge and expertise to meet our customer's needs

Our targets	Our performance		
The minimum standards we expect to achieve	How we did in November	Compared to October	Over each of the last six months (June 2016 to November 2016)
At least 80% of BOI product knowledge reviews are rated green or amber in the quarter	100.0%	0.0%	100% 100% 100% 100% 100% 100%
At least 80% of BOI regulatory awareness reviews are rated green or amber in the quarter	95.0%	-2.1%	100% 100% 100% 97% 97% 95%
Specialists pass at least 80% of POL knowledge tests in the quarter	99.7%	+0.5%	99.2% 99.2% 99.2% 99.2% 99.2% 99.7%

Trends and exceptions

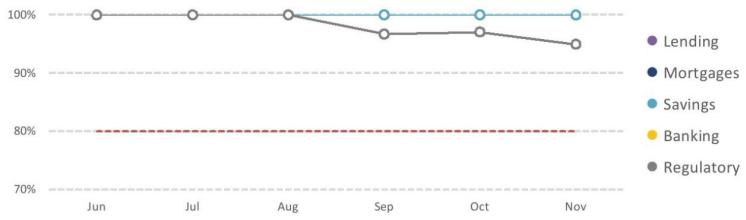
One Directly Managed branch - Haywards Heath - was rated red in relation to regulatory knowledge by the BOI Risk Assurance Team in November. The exceptions noted related to staff knowledge in relation to a complainant's right of FOS referral, the mandatory completion of the POL Regulatory Workbook, staff knowledge of the sales process - in particular, in relation to product comparisons and the provision of financial advice - and staff being unable to locate operational branch procedures. These findings were fedback to the Branch Manager, who was directed to take action to improve the knowledge of staff in these areas.

No other material exceptions or hot spots were identified.

BOI branch knowledge reviews (last 3 months)

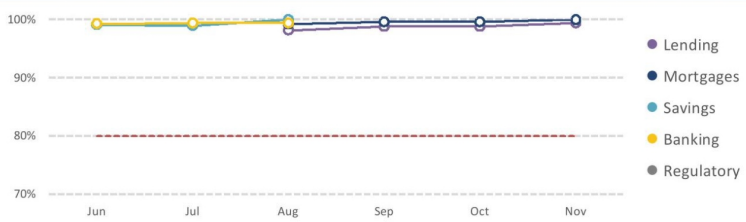
80 staff product knowledge reviews were carried out by BOI during the three months to the end of November. All 80 of these were rated green or amber.

40 staff regulatory awareness reviews were carried out by BOI during the three months to the end of November. 38 of these were rated green or amber and 2 were rated red.



POL Specialist knowledge tests (last 3 months)

324 Specialist knowledge tests were performed by Post Office during the three months to the end of November. 323 of these were passed and were failed.



POL00247018

Appendix to Action POLARC 16/43(e)

Financial promotions and social media

We use branch reviews and monitor breaches to ensure our financial promotions are compliant and up to date, and our social media use is compliant

Our targets	Our performance		
The minimum standards we expect to achieve	**How we did in November**	**Compared to October**	**Over each of the last six months (June 2016 to November 2016)**
90% or more of our branch reviews are rated green or amber for financial promotions in the quarter	98%	▲ +0.4%	100.0% 96.9% 97.1% 93.3% 97.1% 97.5%
We record fewer than 4 material breaches and no systemic issues in relation to financial promotions	4	▼ +3	1 0 0 0 1 4
We record fewer than 7 material breaches and no systemic issues in relation to social media use	3	◀▶ -	0 0 0 0 3 3

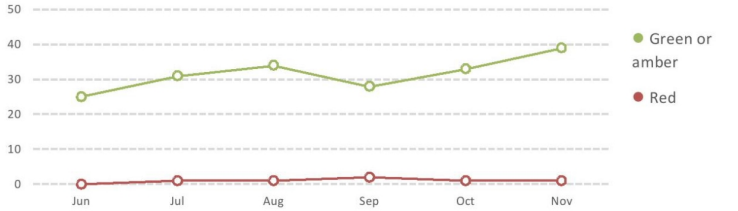
Trends and exceptions

Three material breaches were recorded by the BOI Financial Promotions Team in November:
(1) Balance transfer credit card online material - the FCA contacted the Bank expressing concerns in relation to the promotion of the interest free period on the Post Office Balance Transfer Card. In particular, the FCA questioned the prominence of the warning that any interest free period would be for 'up to' 37 months. Following discussions with Post Office, the material was amended accordingly.
(2) Mortgage 'pay per click' online material - The live version of the material differed to that approved, as a result of errors by the agency. The material was subsequently corrected.
(3) Credit card affiliate online template - The live version of the material differed to that approved. The material has been corrected and the underlying cause of this issue is still under investigation.

No social media breaches were reported by Post Office in November.

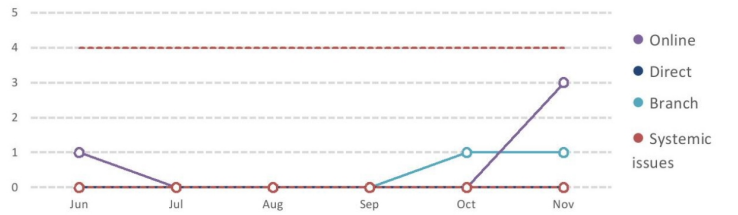
BOI branch financial promotions reviews (branch ratings in last 3 months)

39 of the 40 branches reviewed by BOI in the three months to the end of November were rated green or amber in relation to advertising and promotions and one branch was rated red.

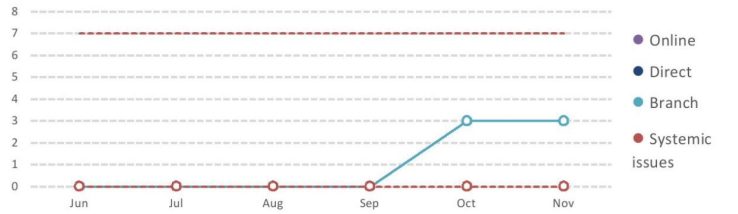


Material financial promotions and social media breaches (last 3 months)

There were 4 material financial promotion breaches reported in the three months to the end of November. There were no systemic conduct issues recorded in relation to financial promotions in November.



There were 3 material scial media breaches reported in the three months to the end of November. There were no systemic conduct issues recorded in relation to social media use in November.



POL00247018

Appendix to Action POLARC 16/43(e)

Product retention and usage

We monitor the retention and use of products by our customers to ensure they meet their needs and expections

Our targets	Our performance		
The minimum standards we expect to achieve	**How we did in November**	**Compared to October**	**Over each of the last six months (June 2016 to November 2016)**
Savings cancellations - Customers cancel no more than 1.5% of savings products in the cancellation period	0.5%	▲ -0.4%	0.8% 0.8% 0.7% 0.7% 0.9% 0.5%
Credit card usage - At least 80% of Matched cards sold in-branch are subsequently used by customers	89%	▼ -1.6%	89.9% 92.1% 91.2% 91.0% 90.3% 88.7%

Trends and exceptions

Savings cancellations - No 'hot spots' or issues identified.

Credit card usage - This KRI has now been updated to reflect the three month usage level of the Matched card only and is rated green. Although still amber rated, usage rates for the Platinum card have slowly improved over the last six months, rising to 74% for November. The C&CRC acknowledges that the Platinum card is primarily designed and promoted for holiday use and that the other management information and KRIs in this regard are not suggestive of systemic branch mis-selling.

Savings cancellations (monthly)

3,657 savings products were sold in-branch in November. Of these, 18 (0.5%) were cancelled by customers during the cooling-off period.

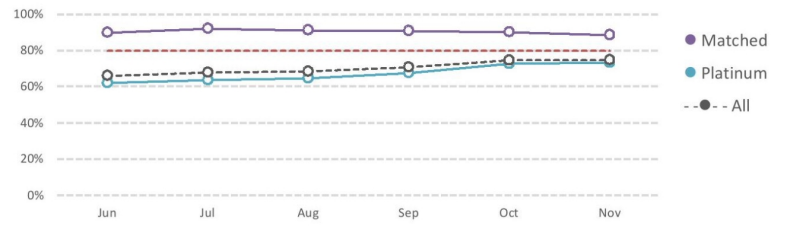
12 (0.6%) of the 1,863 variable rate products were cancelled and 6 (0.3%) of the 1,794 fixed rate products were cancelled.



Matched credit cards used in first 3 months

1,120, or 74.9%, of the 1,496 credit cards opened by branches in the three months to September 2016 have since been used by customers.

73% of the 1,354 Platinum cards opened in-branch in this period and 89% of the 142 Matched cards have since been used by customers.



Last month's performance shown in brackets

POL00247018

Appendix to Action POLARC 16/43(e)

Training and competence

We monitor training and competence to ensure staff maintain their competence and are adequately supervised

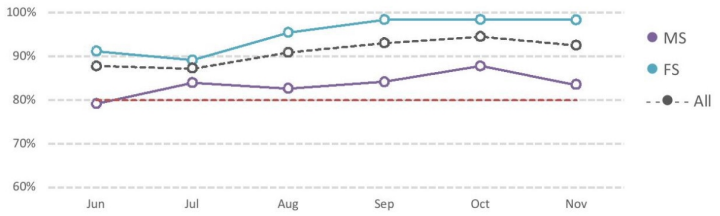
Our targets	Our performance		
The minimum standards we expect to achieve	How we did in November	Compared to October	Over each of the last six months (June 2016 to November 2016)
At least 80% of Specialists are signed-off as competent	93%	-2.0%	87.8% 87.3% 90.9% 93.1% 94.6% 92.6%
At least 80% of FSAMs are within agreed spans of control	96%	0.0%	100.0% 96.0% 96.0% 96.0% 96.0% 96.0%
At least 80% of FSAM reviews are rated green or amber	100%	0.0%	100.0% 95.8% 95.2% 95.2% 100.0% 100.0%

Trends and exceptions

Although within tolerance, the proportion of Mortgage Specialists yet to be signed off as 'fully competent' remains amber rated at 83.5% (66 out of 79). This situation continues to be actively monitored and managed by POL FS Risk T&D, with low levels of sales activity or temporary withdrawal due to non-competence continuing to result in delays in signing individuals off as fully competent. In addition, five new Mortgage Specialists are now under close/enhanced supervision.

Specialists signed-off as fully competent

93% of Specialists have been signed off as fully competent and 7% are subject to close supervision. 2 (2) Financial Specialist are subject to close supervision and the remaining 121 have been signed-off as competent. 13 (9) Mortgage Specialist are subject to close supervision and the remaining 66 have been signed-off as competent.



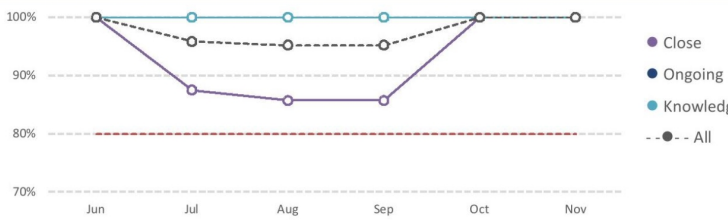
Supervisors within agreed spans of control

24 out of 25 FSAM teams are operating within agreed spans of control under the scheme.



BOI FSAM reviews rated green or amber (last 3 months)

All FSAMs were rated either amber or green for their T&C supervision and knowledge in the BOI reviews performed in the three months to the end of November. no FSAMs were rated red in relation to their 'close supervision', none were rated red in relation to their 'ongoing supervision' and none were rated red in relation to their 'T&C knowledge'.



Last month's performance shown in brackets

POL00247018

Appendix to Action POLARC 16/43(e)

Post Office Money branch distribution key risk indicators

How we measure ourselves

We use a range of primary and secondary key risk indicators to measure our conduct risk performance. Primary indicators are designed to provide direct insight into customer experience and secondary indicators are designed to provide indirect insight into customer experience. We measure each of these indicators on a monthly basis and rate our performance either green, amber or red based on the metrics shown below.

Primary indicators

KRI description		Our metrics and tolerances		
		Within tolerance		Outside tolerance
		Green	Amber	Red
We use **mystery shoppers** to test how well our staff are meeting our conduct risk requirements and our customer's needs	The proportion of shops rated red in previous three months	0.00% - 10.99%	11.00% - 20.00%	20.01% - 100.00%
	The number of shops rated black in previous month	0		1 or more
	The proportion of Specialists with multiple (>1) red/black shops in the previous six months	0.00% - 5.99%	6.00% - 10.00%	10.01% - 100.00%
Our Quality Assurance Team assess the **quality of the mortgage advice** we give customers to ensure it's suitable to their needs	The proportion of mortgage cases rated A or B by the QAT on initial review in the previous month	100.00% - 90.00%	89.99% - 80.00%	79.99% - 0.00%
	The proportion of mortgage cases rated D by the QAT on initial review in the previous month	0.0% - 5.99%		6.00% - 100.0%
	The proportion of Mortgage Specialists with 80%+ A/B grades on initial review in the previous month	100.00% - 90.00%	89.99% - 85.00%	84.99% - 0.00%
We monitor customer **complaints** to understand what we're getting wrong and why, and to ensure we get it right in the future	The number of upheld branch distribution complaints per 100 products sold	0.000 - 0.599	0.600 - 1.000	1.001 or more
	The number of upheld branch advice or information complaints per 100 products sold	0.000 0.160	0.161 - 0.259	0.260 or more
We use **customer feedback** to tell us whether we met their needs at the point-of-sale	The proportion of customer responses to compliance surveys confirming compliance requirements were met at the point of sale in the previous 3 months	100.00% - 95.00%	94.99% - 90.00%	89.99% - 0.00%
	The proportion of customer responses to NPS surveys that confirm adequate information was provided at the point of sale in the previous three months	100.00% - 95.00%	94.99% - 90.00%	89.99% - 0.00%

Secondary indicators

KRI description		Our metrics		
		Green	Amber	Red
We use the results of **knowledge tests** to ensure our staff have the skills, knowledge and expertise to meet our customer's needs	The proportion of 'product knowledge' assessments rated green/amber during BOI branch reviews completed in the previous three months	100.00% - 90.00%	89.99% - 80.00%	79.99% - 0.00%
	The proportion of 'FCA' assessments rated green/amber during BOI branch reviews completed in the previous three months	100.00% - 90.00%	89.99% - 80.00%	79.99% - 0.00%
	The proportion of POL knowledge tests passed by Specialists and FSAMs in the previous three months	100.00% - 90.00%	89.99% - 80.00%	79.99% - 0.00%
We use branch reviews and monitor breaches to ensure our **financial promotions** are compliant and up to date, and our use of socila media is compliant	The proportion of 'advertising' assessments rated green/amber during branch reviews completed in the previous three months	100.00% - 95.00%	94.99% - 90.00%	89.99% - 0.00%
	Material financial promotions breaches recorded in the previous three months	0 - 2	3 - 3	4 or more
	Material social media breaches recorded in the pervious three months	0 - 4	5 - 6	7 or more
We monitor the **retention and use of our products** by customers to ensure they meet their needs and expectations	The proportion of savings products cancelled within the cooling-off period in the previous month	0.00% - 1.00%	1.01% - 1.50%	1.51% - 100.00%
	The proportion of Matched Credit Cards opened in-branch and subsequently used by customers	100.00% - 86.00%	85.99% - 80.00%	79.99% - 0.00%
We monitor our **training and competence** arrangements to ensure staff are maintaining their competence and are being adequately supervised	The proportion of current Specialists signed-off as fully competent	100.00% - 90.00%	89.99% - 80.00%	79.99% - 0.00%
	The proportion of FSAMs within supervisory spans of control	100.00% - 90.00%	89.99% - 80.00%	79.99% - 0.00%
	The proportion of close supervision, ongoing supervision and T&C knowledge related assessments rated green/amber during branch reviews completed in the previous three months	100.00% - 90.00%	89.99% - 80.00%	79.99% - 0.00%

POL00247018

Post Office Money branch distribution - quality of mortgage advice report for December 2016

Appendix to Action POLARIS 16743(e)

Our performance

	This month	Compared to last month	Compared to 6 month average
Initial assessment pass rate	92.1%	100.0% ▼	93.8% ▼
A rated cases	63.5%	71.0% ▼	55.4% ▲
B rated cases	28.6%	29.0% ▼	38.4% ▼
C rated cases	4.8%	0.0% ▲	3.3% ▲
D rated cases	3.2%	0.0% ▲	2.0% ▲
Final assessment pass rate	96.8%	100.0% ▼	98.1% ▼
MS achieving QAT benchmark	84.8%	97.0% ▼	91.0% ▼
MS on 100% checking	30.3%	25.0% ▲	29.7% ▲

Key themes and root causes

- Of the 63 cases assessed by the QAT this month, 58 passed and 5 failed. Of those that failed, 3 were rated C, 2 were rated D and none were rated E.
- 63% of cases were rated A, against a target of 60%.
- 5 Specialists did not achieve the QAT benchmark.
- Of the 63 cases reassessed this month, 61 passed and 2 failed.

Key errors and themes

Top 5 errors this month (number/% of errors)

1	Factfind incomplete (16)	29%
2	Case notes inadequate (13)	24%
3	Suitability letter inadequate (12)	22%
4	Advice inappropriate (3)	5%
5	Inaccurate KFI+, etc (3)	5%
6	Other (8)	15%

Key error areas



The overall pass rate fell from 100% in October to 92% in November, although this is still well above the tolerance of 80%. 64% of cases were rated A, which is above the target level of 60% for the second month in a row. Two cases were rated D in November, where the advice was considered to be unsuitable.

Five of the 31 Mortgage Specialists who had cases checked in November fell below the QAT benchmark, with less than 80% of their cases being rated A or B. However, this figure is significantly distorted by the low number of cases submitted. Of the five Specialists falling below the benchmark, four only submitted one case in the month and the other only submitted two cases. As such, it is recommended that the metric be amended to take account of cases submitted over either a rolling three or six month period. This recommendation will be presented to the C&CRC in December.

BOI UK Classification: Red (confidential)

Regional summary

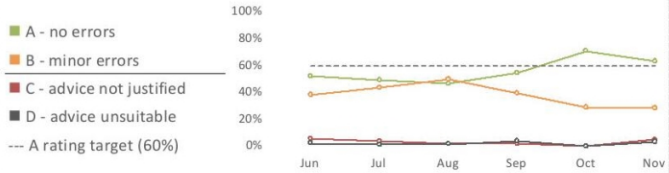
This month (compared to last month)

	North			Central			South		
Initial pass rate	95%	100%	▼				85%	100%	▼
A grade cases	63%	73%	▼				65%	67%	▼
D grade cases	2%	0%	▲				5%	0%	▲
MS at benchmark	89%	100%	▼				80%	92%	▼

Initial assessments

63 initial assessments were completed by the QAT this month.

Monthly rating distribution



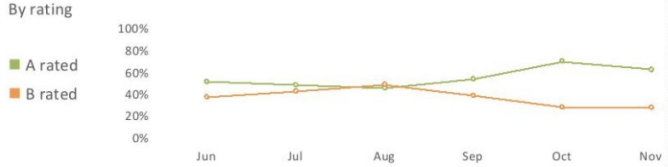
Cases passing the QAT check

92% of cases passed the initial assessment. 40 (63%) were rated A, where no errors were identified, and 18 (29%) were rated B, where minor errors were identified.

By region

		Jun-16	Jul-16	Aug-16	Sep-16	Oct-16	Nov-16
North	Pass rate	92%	90%	97%	97%	100%	95%
	A rated	46%	50%	49%	65%	73%	63%
	B rated	45%	40%	49%	29%	27%	33%
Central	Pass rate	86%	96%	91%	100%	######	
	A rated	57%	46%	45%	62%	######	
	B rated	30%	50%	45%	45%	######	
South	Pass rate	95%	100%	100%	78%	100%	85%
	A rated	65%	55%	42%	11%	67%	65%
	B rated	30%	45%	58%	50%	33%	20%

By rating

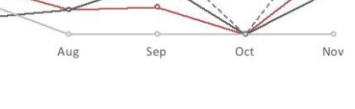


Cases failing the QAT check

5 cases, accounting for 8% of those reviewed, failed the initial QAT assessment. Of these, 3 were rated C, where the advice could not be confirmed as suitable without further information, 2 were rated D, where the advice was considered unsuitable and none were rated E.

By region

		Jun-16	Jul-16	Aug-16	Sep-16	Oct-16	Nov-16
North	Failure rate	7.0%	6.0%	2.9%	3.2%	0.0%	4.7%
	C rated	4.2%	4.0%	2.9%	0.0%	0.0%	2.3%
	D rated	2.8%	2.0%	0.0%	3.2%	0.0%	2.3%
Central	Failure rate	10.8%	3.8%	9.1%	0.0%	#DIV/0!	
	C rated	8.1%	3.8%	0.0%	0.0%	#DIV/0!	
	D rated	2.7%	0.0%	9.1%	0.0%	#DIV/0!	
South	Failure rate	5.0%	0.0%	0.0%	22.2%	0.0%	15.0%
	C rated	5.0%	0.0%	0.0%	11.1%	0.0%	10.0%
	D rated	0.0%	0.0%	0.0%	11.1%	0.0%	5.0%

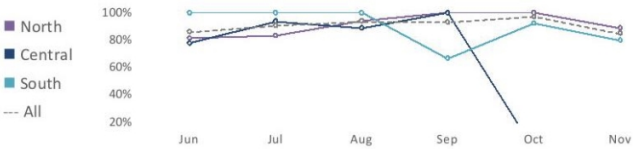


By rating

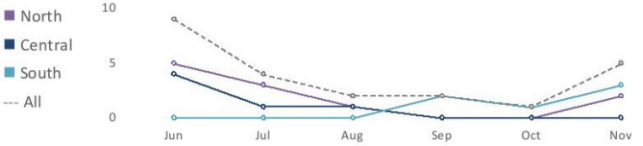
QAT benchmark

85% of Specialists met the QAT benchmark, which is to have at least 80% of their cases rated A or B in the previous 3 months. 5 Specialists did not achieve this benchmark.

Specialists meeting the QAT benchmark



Specialists not meeting the QAT benchmark



POL00247018

Post Office Money branch distribution complaints report for December 2016

Appendix to Action POLARIC 16/43(e)

Our performance

	This month	Compared to last month	Compared to this time last year
Complaints logged	53	44 ▲	95 ▼
Complaints closed	66	78 ▼	116 ▼
Compensation paid	£3,763	£3,339 ▲	£11,768 ▼
Complaints upheld by BOI	74.2%	80.8% ▼	81.9% ▼
Closed within 8 weeks	59.6%	59.5% ▲	74.6% ▼
Upheld per 1,000 sales	0.73	0.65 ▲	
Average compensation	£77	£53 ▲	£124 ▼
Complaints upheld by FOS	1	0 ▲	1 ▲
Cases referred to FOS	3	0 ▲	4 ▼

Key themes and root causes

Key reasons for upheld customer complaints in the last 3 months

		Upheld/Closed
1	Document certification process	85/88 (97%)
2	Application errors (e.g. incomplete/missing forms)	27/31 (87%)
3	Transactions (e.g. lodgements not credited)	19/25 (76%)
4	Experience (e.g. branches not accepting cheques)	21/30 (70%)
5		

Levels of branch-related complaints logged rose slightly in November, but continued on a downward trend over the last 12 months. Complaints categorised by the BOI Customer Care Team (CCT) as relating to document certification, application errors and in-branch transactions continue to account for a significant proportion of complaints logged and upheld. Certification complaints closed in November related predominantly to Credit Card and the majority of these - 97% - were upheld.

Branch advice and information related complaints continued at very low levels, with only one information complaint being upheld and no advice related complaints being upheld in November.

Product summary

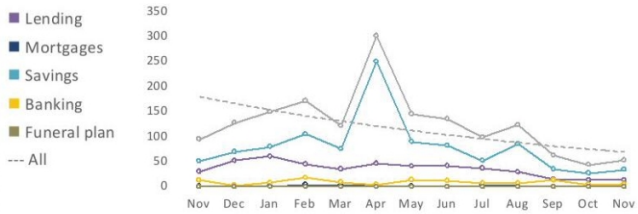
This month (compared to last month)

	Lending		Mortgages		Savings		Banking		Funeral plan	
Logged	**13**	13	**1**	0	**34**	27	**5**	4	**0**	0
Closed	**13**	26	**0**	0	**43**	42	**10**	10	**0**	0
Upheld	**85%**	85%	**0%**	0%	**70%**	74%	**80%**	100%	**0%**	0%
Avg redress	**£35**	£47			**£95**	£55	**£66**	£23		

Complaints logged

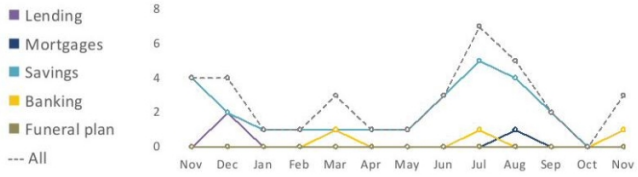
Number of complaints logged

Monthly by product area

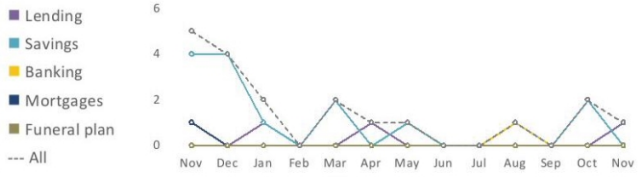


FOS referrals

Complaints referred to FOS



Complaints upheld by FOS

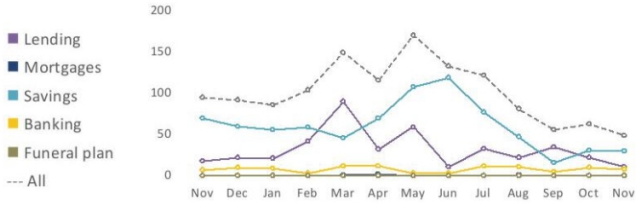


Complaints closed

66 branch complaints were closed this month, 49 (74%) of which were upheld in the customer's favour. £3,763 in compensation was paid out, an average of £77 per complaint.

Number of complaints upheld by BOI

Monthly by product area



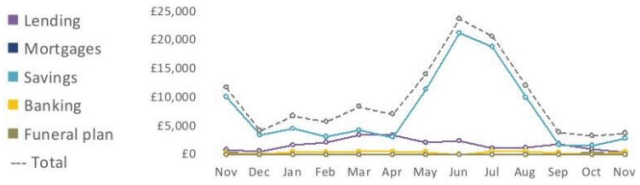
Proportion/number of complaints upheld by BOI

By product area (this month v previous 12 months)



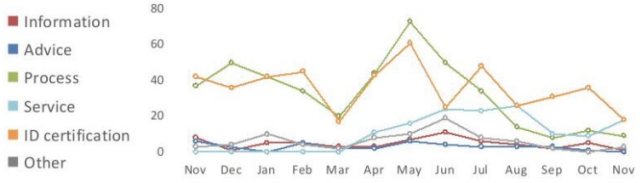
Compensation paid by BOI

By product area



Complaints upheld by BOI

By reason for complaint



BOI UK Classification: Red (confidential)

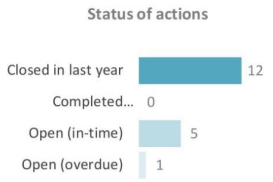
POL00247018

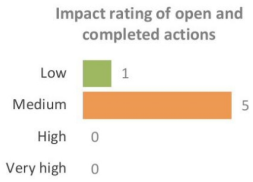
Issues and actions

Appendix to Action POLARC 16/43(e)

Action summary

There are currently 6 open actions, one of which is overdue, and no completed actions awaiting closure. 12 actions have been closed in the last 12 months. Of the open actions, none are very high impact, none are high impact, 5 are medium impact and one is low impact.











Live action update

Potential customer impact	Our progress	Ref	The date the issue was raised	The issue we identified and the impact on customers	The actions we're taking	The owner of the actions	When we expect to complete the actions	The current status of the issue
●	●	001	31-Mar-16	**Current Account downgrade processes** - A root cause analysis of Post Office Current Account related complaints and mystery shops highlighted concerns in relation to the process by which customers are 'downgraded' from standard to control accounts, both at the point-of-sale and thereafter.	The post-application referral process has been reviewed and a number of potential causes of customer complaint (and potential process improvements) have been identified. These are being followed up with the Product Team. Given the nature of the potential process/system improvements required the deadline date has been further extended to the end of December.	BOI/POL Product Teams	31-Dec-16	Open
●	●	002	31-Mar-16	**Improving complaints related communications between BOI and POL** - Following feedback from BOI GIA and POL FS Risk in relation to gaps in complaint MI, work is being taken to improve access to the PO branch network for the BOI Customer Care Team.	Complaints reporting between BOI and POL has now been improved and the BOI Customer Care team have made process changes designed to improve the identification of the branch/Specialist concerned at the point of complaint. Work continues to find ways of improving access to the branch network for BOI and POMS complaints handlers. While having an additional 'single point of contact' resource within POL cannot be justified, other existing POL processes may provide a viable alternative solution and a further meeting is planned for January.	POJV Compliance/POL Risk/POL Ops/BOI Customer Care Team	31-Jan-17	Open
●	●	005	31-Mar-16	**Internal staff incentives and competitions** - Concerns have been raised by BOI Conduct Risk, as 'conduct templates' are not completed by POL in relation to internal staff incentives and internal/customer competitions.	Structural changes in Post Office have resulted in a delay to the resolution of this matter. Bob Tennant is currently reviewing the situation before deciding what, if any, further action needs to be taken by POL.	Bob Tennant	31-Oct-16	Open
●	●	006	31-Mar-16	**Post-sale document certification and AML ID verification complaints** - Despite various communications to the network, customer complaints in relation to post-sale document certification and AML ID verification have not reduced.	A joint BOI/POL action plan is in place. Progress against the action plan is being reported to the C&CRC on a monthly basis. Outline proposals have been made by POL to agree which branches can provide ID certification services, and to reflect these on the branch services list and the POL website. These proposals are now awaiting approval from the POL Network Team before being finalised. A proposal for aligning post-sale customer correspondence with this is also under consideration.	POL Risk/POJV Compliance/DMLRO	31-Dec-16	Open
●	●	008	01-Jul-15	**Incomplete Mortgage Specialist qualification and fitness and probity records** - POL T&D have identified significant gaps in the qualifications and fitness and probity records maintained by POL HR in relation to a number of Mortgage Specialists (MSs) and the FSAMs that supervise them.	A review conducted by BOI Risk Assurance was rated red and highlighted signficant concerns in relation to the deployment, quality control and oversight of F&P processes by POL HR. Revised systems and controls have now been put in place to mitigate the risks identified, and BOI Risk Assurance have reviewed the actions taken by POL and have closed their review. A follow-up review will take place in early 2017.	POL Risk		Closed

POL00247018

Appendix to Action POLARC 16/43(e)

Potential customer impact	Our progress	Ref	The date the issue was raised	The issue we identified and the impact on customers	The actions we're taking	The owner of the actions	When we expect to complete the actions	The current status of the issue
●	●	012	01-Oct-16	**Mortgage Adviser competence (previously 'validating mortgage customer preferences')** - Continued red-rated mystery shops have highlighted ongoing challenges in relation to the maintenance of Mortgage Adviser competence, when activity levels are low.	Red-rated Mortgage shops continue to be a cause for concern and there remains a concern that the actions taken to date have not provided a long-term solution to this issue. As such, a further action plan, designed to ensure that Mortgage Specialists maintain competence in periods of low productivity, was approved by the Customer and Conduct Risk Committee in November 2016. The impact of this will be monitored over the next 3-4 months. Accordngly, the deadline for this action has been extended to the end of March 2017.	PO FS sales	31-Mar-17	Open
●	●	020	03-Oct-16	**Sales support material** - Two recent instances where 'sales support' material was used without being approved in advance have highlighted a need for us to tighten up/extend our procedures in this regard.	Post Office have included requirements and guidance in this regard in their new Conduct Compliance Manual, which is due to be distributed to the network in December 2016.	POJV Compliance	31-Dec-16	Open

POL00247018

Appendix to Action 1642(i) EUM Update to ARC

Enhanced User Management Update to ARC – January 2017

The EUM project is making good progress across the core streams of funding, solution build/implementation and audit:

Funding

- The EUM Delivery programme budget has been ratified by POL ESG, with a recommendation going to the POL Board in January 2017 to approve the £7.8m investment. This encompasses EUM build and delivery execution across the wider branch network.

Solution build and implementation

- A working prototype of the EUM core software (that regulates user access to transaction processing systems) is available and key functionality has been demonstrated to stimulate final shaping of the system minimal viable product (MVP). MVP product build and user acceptance testing, which are being achieved using an agile approach, will be completed by February 2017.
- In parallel, activity is underway to execute data cleansing (of vetting and training data from legacy repositories) and to design the integration with Success Factors for user vetting and training/competency management
- The programme is on schedule to commence a 25 branch pilot in March 2017 with full network rollout occurring in July 2017.
- Full network rollout of EUM capability is still to be planned, but is expected to be completed by November 2017.

Audit

- POL Legal has completed a review of the top 20 POL contracts (including those associated with the Banking Framework, POMS and for Bank of Ireland) to ensure that all obligations relating to vetting/training (principally compliance and audit orientated) will be satisfied by the future EUM system and enhanced business processes. The conclusion is that EUM as defined will addresses obligations for these contracts.
- A 50 branch desk audit across a sample of directly managed and agency branches has been completed by POL Internal Audit to assess the efficacy of existing record keeping for vetting and training records. While the work is scheduled to deliver in January, early findings confirm that existing data capture and record retrieval processes for agency branches (the key concern for POMS and Banking Framework) are operating satisfactorily.

Conclusion:

- The project is making good progress and is on track to deliver a robust, long term solution for Post Office.
- The positive audit results in agency branches, combined with the wider project status and other actions being undertaken by POMS, should enable POMS management to recommend to the POMS board at its January meeting that, while the sales processes remains outside appetite, there is an evident route to achieving appetite within a reasonable timeframe; as such I would have confidence that the POMS board would support the continued sale of travel insurance in agency branches while the project is fully implemented; following the rollout of a new protection model in January, life assurance sales will be restricted to a limited number of branches, thereby significantly limiting the risks associated with this product).

POL00247018

Financial Reporting Controls Update

Author: Danielle Goddard Sponsor: Al Cameron Meeting date: 30 January 2017

Executive Summary

Context

As advised to ARC in 2016, the focus is on implementing a Financial Controls Framework ('FCF') that is fully operational by the end of the financial year, and embedded in a sustainable way.

The build of the Financial Controls Framework is substantially complete and it is now becoming operational. The purpose of this paper is to update the ARC on progress and next steps.

Questions addressed in this report

Building the Framework

1. What has changed since the last ARC?
2. What is the status of the high risk control gaps?
3. What further progress is required for the build of the Financial Controls Framework to be complete?

Operating the Framework

4. How much of the Financial Controls Framework has been self-assessed to date and what are the results?
5. What independent review has been performed to date and what are the results?
6. What further work and testing is planned?

Other

7. What other control improvements are planned or in progress?

Conclusions

The Financial Controls Framework is expected to be fully operational by end March, with reliance available through 2017/18. Obviously, controls will continue to be assessed, developed, and improved next year.

62% of remediation is now complete with 42 control gaps remaining. Control self-assessment using the PwC developed tool TrAction has now been rolled out for 11 of the 12 processes completed to date.

In December, 56% of controls were issued for self-assessment. 79% of these were self-assessed without exceptions.

POL00247018

We expect all currently identified remediation to be complete and every control to have been through at least one round of self-assessment by the end of the financial year. Each process will also have had a sample of controls independently assessed at this point.

We will begin documentation of Masterdata controls in February 2017, with control gaps expected to be identified and remediated (at least with work-around controls) by the end of the financial year.

Input Sought

The ARC is asked to note the progress made and comment on the priorities and approach.

The Report

Building the Framework

1. What has changed since the last ARC?

1.1. Overall, 276 key controls have been identified for us to rely on, down from 291 at the November ARC, as controls are confirmed and duplicates removed.

1.2. Of these 276 controls, 42 have some gaps, reduced from 110 at November. 7 are high risk (reduced from 9), 16 medium, and 19 low risk. An update is provided below on high risk control gaps. 11 of the 12 identified processes now have controls on our self-assessment tool. The first process has been assessed by PwC; no significant issues emerged.

2. What is the status of the high risk control gaps?

2.1. We originally identified 10 high risk control gaps, of which 3 are fully closed.

2.2. The high risk gap in relation to reconciliation of branch cash between Horizon and POLSAP has been closed for Sterling branch cash but is open for other elements of network cash.

POL00247018

2.3. Status of high risk gaps:

High Risk Gap	November ARC	January ARC	Year end - expected
Period end checklist	In progress	Closed	Closed
Authorisation of manual journals	In progress	Closed	Closed
Monthly FLT balance sheet review	In progress	In progress	Closed
Independent review of monthly balance sheet probity	In progress	In progress	Closed
Reconciliation of branch cash between Horizon and POLSAP	Closed (Sterling branch cash)	Closed for Sterling branch cash; in progress for other elements of network cash.	Closed
Review of goods receipting	In progress	In progress	Closed
Payroll segregation of duties	In progress	In progress	Closed
Central review and quality of bank reconciliations	In progress	Closed	Closed
Quality of balance sheet reconciliations	In progress	In progress	Closed
Spreadsheets policies and controls	In progress	In progress	Closed

2.4. See Appendix 1 for detail of all open and closed high risk gaps.

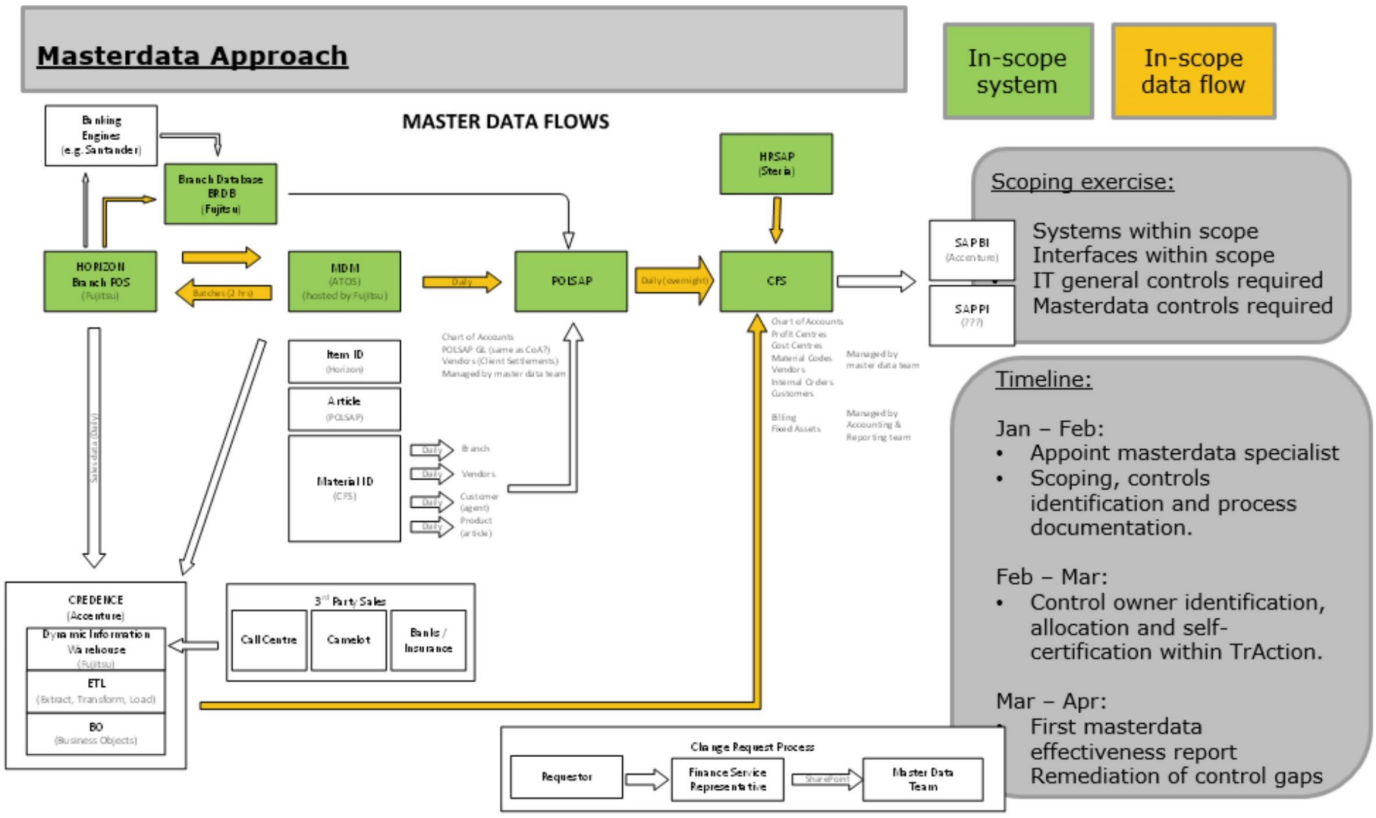
3. What further progress is required for the build of the Financial Controls Framework to be complete?

3.1. The build of the Financial Controls Framework is substantially complete and the following work is planned to fully complete it by the financial year end:

a. Remediation of the remaining 42 control gaps.
b. Identification of control owners for 16 unassigned controls. These are typically automated controls without a natural owner.
c. Uploading of the remaining process, Control Environment, in the Self-Assessment tool.
d. Quality review; internal review via a weekly forum, and external review through PwC sample testing.
e. Masterdata; Progress on masterdata controls has been delayed due to lack of available suitable resource. We have now recruited a specialist who will document the masterdata processes and controls from 1 February. The process of documentation, identification and remediation of control gaps is expected to be complete by the end of the financial year but this may rely on work-around

POL00247018

controls pending the Back Office Transformation. The diagram below shows an overview of the relevant systems and masterdata and our planned timeline.



3.2. We will also complete areas not included in the original scope; Agents' Debt, Branch Corrections Process, Agents' Remuneration, and POMS. This work will commence in March 2017. Note that a separate internal audit review of POMS controls was performed in FY16/17, with no significant issues identified.

POL00247018

Operating the Framework

4. How much of the Financial Controls Framework has been self-assessed to date and what are the results?

4.1. The December 2016 self-assessment results are shown below. Further detail by process is shown within the table in Appendix 2.

Total controls	**276**	
Less: Controls in remediation	-42	
Controls to be assigned	-16	
Controls to be set to live	-31	
Controls not due to be operated due to frequency	-32	
Total population for self-assessment	**155**	**56%**
Self-assessed and operated effectively	123	79%
Self-assessed but not operated effectively	18	12%
No self-assessment submitted	14	9%
Population for self-assessment which has been independently tested	**7**	**5%**

4.2. Exceptions and comments from the December 2016 self-assessment have been reviewed and there are no items which cause concern, conversations are underway to enable control owners to operate controls they consider effective. In the 14 cases where no self-assessment was made, manager conversations are underway. Repeated omissions will lead to disciplinary action.

5. What independent review has been performed to date and what are the results?

5.1. PwC has been engaged to perform independent sample testing of the Self-Assessment and control evidence, split into 4 phases. Phase 1 was testing of Client Settlements and this was performed in December 2016; of the 7 controls tested, PwC recommended some minor risk and control description changes which we have accepted. They did not identify any key weaknesses during their review.

5.2. PwC's findings on testing of the Client Settlement process is summarised below.

Total Client Settlements controls	**13**	
Total controls tested	7	54%
Concluded as operating effectively	7	100%
Concluded as not operating effectively	0	0%

POL00247018

6. What further work and testing is planned?

6.1. The remaining PwC testing is being completed as follows:

a. Phase 2 - w/c 23 January 2017; Project Accounting, Fixed Assets, Record to Report, Payroll, Tax.

b. Phase 3 – w/c 20 February 2017; Stock, Bill to Cash, Procure to Pay, Treasury, Bank & Cash, Control Environment.

c. Phase 4 – w/c 3 April 2017; Quarter 4 and Annual controls for the above processes.

6.2. We also plan to perform further review internally and have set up a weekly Quality forum, as well as continuing with gathering evidence for all controls for quality review purposes.

7. What other control improvements are planned or in progress?

7.1. We are working together with IT to ensure that the control weaknesses identified in the FY2015/16 EY IT audit are incorporated into the IT Controls Framework; some remediation has been performed since last year end, but each of the weaknesses identified will be addressed as part of the IT Controls Framework to ensure that sustainable remediation is implemented.

7.2. In December we implemented a monthly review of all incident escalations one month in arrears. The review is performed within the Financial Control team and assesses each incident for; potential financial impact, risk of misstatement, risk of fraud, and risk of non-compliance with laws and regulations. This will be communicated monthly to EY.

7.3. As noted in the incident report to the ARC, Finance has highlighted a number of incidents where, while we do not believe there has been any financial statement impact, we need to provide positive assurance. This work will be undertaken with EY.

POL00247018

Appendix 1

7.4. The following high risk gaps have been closed since November ARC:

High Risk Gap	Progress
The period end checklist does not cover the full set of accounts, tasks and dependencies	**Status: Closed.** Period end checklist was fully operational in Period 9. A full period end checklist was created covering all 252 period end tasks split by process. Task owners were trained and the checklist was fully operational in Period 9. The Period 9 ledgers were not closed until the Financial Control team were comfortable that all pre-close tasks had been completed or mitigated. The Period 9 response rate was 81% with 19% mitigated through additional checks. 13% were non-responses regarding completeness of manual journal submissions. We have addressed non-conformance through follow up communications and expect an improvement for Period 10.
Journals receive a sense check versus previous months but are not formally approved	**Status: Closed.** Journal authorisation policy was fully operational in Period 9. Manual journal requests now require authorisation from an approved authoriser if they have a P&L impact of £250k, or a balance sheet impact of £1m. Requests for manual journal reversals also require approval. The approval is evidenced with an audit trail via a Journal Authorisation Sharepoint site. This process has been trialled for a number of months, and was complied with by 100% of journal providers for Period 9. In Period 9, 30% of manual journals met the materiality threshold and 100% of these were independently authorised. Only 2% were initially received without proper authorisation, and these were rejected and followed up. Upon a quality review of the control by the FCF team, we had the following concerns and plans to address them: Potential for the journal provider to change the journal between approval and processing; sample of 25 was tested after period end to ensure that the journal processed was authorised. One exception was identified and this issue is being followed up. Completeness of manual journals; rejected journals were followed up before the period was closed to ensure that a replacement journal had been received and processed.
No central review and quality check of bank reconciliations	**Status; Closed.** All bank reconciliations are being reviewed centrally on a monthly basis, with any issues being reported and resolved each month. The quality has improved significantly since the central review and training has been performed.

7.5. The following high risk gaps currently remain open as at the date of this paper:

High Risk Gap	Progress
Goods receipting is done inconsistently with limited reviews of open purchase orders	**Status; In progress (owner: Financial Controller)** January update: A monthly review of all open 3 way match purchase orders has now been implemented but response rates have been low so far. In order to cleanse the data, a total of 2,979 WBS codes were closed relating to old projects. Owners were confirmed for all remaining projects and agreed with Finance Directors.

POL00247018

	An open Purchase Order report was issued for review during Period 8 and Period 9. In Period 9 out of a total 571 purchase orders to be reviewed, 196 (34%) were reviewed. A communication has been issued by the Financial Controller in order to encourage an improved response for Period 10 onwards. The Financial Control team will continue to perform a monthly central review and manual adjustment of GRIR until this is fully embedded. However, the additional review appears to have already increased the accuracy of goods receipting; the level of manual adjustment required has reduced from Period 7 by 48% (£1.56m) in value, and 10% (11) in volume.
Monthly balance sheet probity reviews by the central Finance team are not signed off by the Finance Directors for each area	**Status: In progress (owner: FLT)** January update: A review and sign off process is now in place, with full sign off expected by the financial year end. A monthly review file has been developed which contains higher risk balance sheet items and exceptional items, split by Finance Director pillar. This file has been issued since Period 7. A monthly meeting has been set up with the FLT, for them to report the results of their review to the CFO. The first review meeting was held on 10 January; some reviews had been completed and others were in progress. The follow-up meeting is scheduled for 23 January. We recognise that it will take a number of iterations for a full local sign off to be achieved, which we expect by year-end.
Balance sheet probity reviews are not independently reviewed	**Status: In progress (owner: Financial Controller)** January update: Requirement to evidence independent review has been communicated and will be mandatory from Period 10 (January 2017). A list of reconcilers and reviewers for each balance sheet GL has been identified. A communication has been issued to notify them that all probity returns must have been reviewed before submitting to the Financial Control team, and that review must be evidenced on the probity form. This will be mandatory from Period 10 and a sample check will be performed to ensure that review was evidenced.
Lack of segregation of duties between staff updating payroll master data and staff processing the payroll	**Status: In progress (owner: Head of Shared Services)** January update: The duties will be split as a priority. We are working with Steria on a HRSAP systems fix, and with the Success Factors project team to ensure sufficient segregation of duties is in place going forwards. In the intervening period a mitigating control is being performed and reviewed centrally. Until the systems solution can be implemented, a mitigating control has been performed whereby all payroll masterdata changes are reviewed to ensure that none were made by the same individuals who processed payroll. The control and evidence has been signed off by the Head of Support Services and also by the Financial Control team. As noted in the incident report, too many people with payroll access rights were identified. This is being corrected, however until the systems solution is implemented a monthly system report has been run to identify and review all users who have accessed the payroll transaction.

POL00247018

Balance sheet reconciliations of variable quality	**Status: In progress (owner: Financial Controller)** January update: Training is in progress and full Balance Sheet reconciliation review expected to be complete by end February 2017. Training has been completed for all areas of the Balance Sheet where required. Due to remaining quality issues, we are performing a full review of all Balance Sheet reconciliations and issuing further training on a 121 basis with formal documentation. This is currently being performed with a target completion date of end February 2017.
Policies to manage and control spreadsheets are inconsistently applied	**Status: In progress (owner: Phil Birds)** January update: The scope of this review has widened. All spreadsheet control recommendations have been identified and are in the process of implementation with an expected completion date of end March 2017. The initial scope of 40 key spreadsheets has been widened to include 134 spreadsheets. This covers all spreadsheets which have an impact on manual journals or billing documents. This is substantially complete with only 6 journals left to review with an expectation of fewer than 6 spreadsheets supporting those journals. An extensive review process has been undertaken broken down into 2 phases as described below. Phase1 (supported by KPMG and Financial Control Team Chesterfield): Tracked all 134 spreadsheets, created a SharePoint site and lead schedule for each spreadsheet. Each spreadsheet was reviewed against set criteria including version control, secure access, and consistency of outputs and built in checks. Notes and recommendations were made for all material spreadsheets which comprised the majority under review. Phase 2: This phase involves formal communication, feedback and recommendations to all spreadsheet preparers supported by KPMG led training days (beginning 13 January) to augment Post Office spreadsheet skills and empower spreadsheet preparers to improve the veracity of their outputs. Finally a process of monitoring and control is being be developed to ensure initial improvements are sustainable going forwards.
Branch cash balances are not routinely reconciled between POLSAP and Horizon	**Status: In progress (owner: Financial Controller)** January update: This gap was previously closed for Sterling branch cash after a monthly branch cash reconciliation was implemented. The gap is open to ensure we reconcile the entire Network cash balance (including foreign currency, cash in cash centres, and cash in ATMs). Horizon reports are being obtained for the remaining element for this to be reconciled monthly going forwards.

POL00247018

Appendix 2

7.6. The following table shows detail of the December self-assessment results, as summarised in section 4.1.

		Control Gaps				Control Owners		December CSA results						
Financial Statement area	Total controls	Total control gaps	H/M/L impact of gaps			Owner assigned	No owner assigned	Control operated effectively	No self-assessment submitted	Not operated due to agreed frequency	Control not operated effectively	Control to be set to live	Evidence quality review performed	PwC testing performed
Bill to Cash	21	3	0	1	2	18	3	8	0	2	3	2	Feb	Feb
Client Settlements	13	1	0	1	0	11	2	8	0	0	0	2	Yes	7
Bank & Cash Management	33	6	1	2	3	32	1	16	0	2	5	3	Feb	Feb
Procure to Pay	26	2	1	0	1	26	0	18	1	0	4	1	Feb	Feb
Project Accounting	11	0	0	0	0	11	0	6	2	2	1	0	Yes	Jan
Fixed Assets	19	3	0	0	3	19	0	11	0	4	0	1	Yes	Jan
Record to Report	39	8	3	4	1	39	0	23	2	3	2	1	Yes	Jan
Stock	18	2	0	1	1	8	10	3	1	1	1	0	Feb	Feb
Payroll	36	6	1	3	2	36	0	19	8	1	0	2	Yes	Jan
Treasury	14	0	0	0	0	14	0	7	0	5	1	1	Feb	Feb
Tax	17	0	0	0	0	17	0	4	0	12	1	0	Feb	Jan
Control Environment	29	11	1	4	6	29	0	0	0	0	0	18	Feb	Feb
ITGCs / MDCs	TBC	TBC				TBC	TBC	TBC	TBC	TBC	TBC	TBC	TBC	Not in scope
Total	**276**	**42**	**7**	**16**	**19**	**260**	**16**	**123**	**14**	**32**	**18**	**31**		
		15%					**6%**	**45%**	**5%**	**12%**	**7%**	**11%**		

POL00247018

Network Conduct Risk Action Plan

Author: Owen Woodley
Meeting date: 30th January 2017

Executive Summary

Context

This paper updates the Committee on progress against the Network Conduct Risk Action Plan. The Action Plan was created by the Financial Services Risk team, in conjunction with Network, to mitigate potential conduct risks related to the sale of financial products and services within the branch network. It address the challenges highlighted by the joint Bank of Ireland and Post Office risk assessment undertaken in 2015, most of the actions have been completed and progress is reported here on the residual items.

Questions this paper addresses

1. What progress has been made against the plan?
2. What is still outstanding?
3. What are the next steps?

Conclusions

1. Good progress has been made against the action plan. We intend to fold this plan into BAU conduct risk activity by the end of the financial year.
2. Staff vetting enhancements and the EUM project will continue to require separate project resource and oversight.

Input Sought

The R&CC is asked to note these developments.

The Report

Key updates and progress made on residual items since the last meeting

1. Sales Model

   Sales models were seen as a risk in the risk assessment, as they could drive inappropriate behaviours in the network. The work in this area is now complete following the actions undertaken by Agency. The Agency sales model for branches with Customer Relationship Managers (CRMs) was re-articulated following a review by the FS Risk team and this has been re-trained out to all Agency RMs and ASPMs.

2. Incentive Schemes

POL00247018

As part of the CRM programme we train out the importance of not putting in place local unapproved incentive schemes and the importance of the regulatory requirements. We also require Postmasters in all CRM branches to sign a declaration agreeing not to set up local incentive schemes.

As part of the residual work to mitigate the risk of unapproved incentive schemes operating in the wider Network (which we would regard as being of low likelihood) A communication to the network (branch focus) re-iterating the importance of not having unapproved local incentive schemes in place will take place in January. This requirement is also articulated in the newly approved conduct compliance manual which is being circulated in the network (see 6 below).

A wider review has been undertaken by the network on all network related incentive schemes to understand their efficacy. Whilst this has highlighted some potential improvements that should be made to the schemes, no new conduct risks were uncovered. A final version of this review will be shared with the risk team in early February for the recommendations to be considered and future governance to be reviewed.

3. Compliance Monitoring

As part of the gap analysis review of compliance monitoring, it was identified that the sales of Travel Insurance, Over 50s Life Insurance and some savings journeys did not have any counter monitoring activity. As a result of these findings a programme of mystery shopping was designed and this began in November 2016. We are working through the initial findings with our regulatory Principals during January.

4. Training

The 'Developing a Great Customer Experience' CBT training programme has been updated and approved to be used for those managers in network and FS who may not have received front line 'customer' training but may need to be aware of conduct risk in their roles in product distribution or design. This training covers regulation, performance management, vulnerable customers and conduct risk for these populations. Next steps are to agree the network delivery plan with FS risk and Success Factors during January.

5. Management Information in the network

There is comprehensive MI in place covering the activities of Specialists and CRMs. For the remainder of the network there is Quality of Sales MI that is sent to the Network management teams on a monthly basis. This covers branch 'watch list' information related to sales spikes, cancellations and complaints.

The Network and FS Risk team have significantly improved the presentation of this management information into a dashboard format so that it is clearer for the Network management teams to identify trends in their area. This improved format will also improve risk oversight of the Network and improve intelligence for monitoring activity.

POL00247018

6. Compliance Manual

Work has been completed to simplify the two Regulatory Guidance Manuals (BoI and POMS) into an easy-to-read guide for staff. The conduct compliance manual has been completed, approved by both Principals and circulated to network.

7. Personal objective setting for senior managers

A review of objectives has been undertaken to ensure that a suitable conduct and compliance objective is in place for all relevant managers and their teams. All were found to have a satisfactory objective relating to compliance. The link to conduct and customer outcomes, however, was less clear. For this reason, wording will be included in the updated version of the conduct compliance manual for the next financial year, covering customer conduct in relation to objectives for managers.

Key issues outstanding

8. Evidence of compliance training in the branch network (EUM Project)

Specific financial services compliance training and testing is provided on Horizon, covering areas including Financial Services requirements, AML and Data Protection. Product training is also provided via distance learning modules. All of these modules are regularly refreshed by Post Office and approved by our Principals. However, we cannot currently provide specific evidence that counter colleagues have taken and passed the requisite modules.

We are working with the IT and Network Support teams to build a solution involving enhanced user access controls on Horizon. These will interact with the new 'Success Factors' training suite, which will provide all training materials.

The enhanced functionality will refuse Horizon access unless an individual has passed the requisite training. Furthermore, it will not allow an individual 'log in' for Horizon to be generated unless that individual has been approved by Post Office HRSC, in line with the HR vetting checks. This project is being classed as high priority. (Nick Kennett sponsor June 2017)

9. Staff vetting (EUM Project)

Whilst all staff, including postmasters' assistants, are CRB-checked, Post Office is introducing more detailed requirements for staff vetting, including credit checks. This is a particularly important requirement for the Banking Framework. As part of the EUM project the enhanced staff vetting process is planned to subsequently interact with 'Success Factors' to ensure that access to Horizon is blocked until that individual has passed vetting. The initial vetting enhancements are planned to be in place from the end of February 2017, but the precise implementation date is still to be agreed (Martin Kirke HR, TBC).

10. Whistleblowing 'Speak Up' policy

POL00247018

The communication plan for the recently-updated Post Office 'Speak Up' policy is still being developed by Corporate Services. Post Office needs to ensure that the policy is communicated appropriately to both employees and agents, taking into consideration that we cannot offer Public Interest Disclosure Act protections to non-employees. (Corporate Services date TBC).

Next Steps

We continue to report progress on the plan monthly at the BOI Customer & Conduct Risk Committee and to the POMS Risk and Compliance Committee as well as to this committee.

POL00247018

Safety

Authors: Martin Hopcroft Sponsor: Angela Van Den Bogerd/Al Cameron Meeting date: 30th January 2017

Executive Summary

Context

1.1 The ARC requested a regular update on our management of risks around the safety of our people and customers.

1.2 Safety performance is reported monthly to the Group Executive and at each Board meeting, together with information on health and wellbeing.

1.3 Accountability for safety has just transferred to Operations from HR, recognising that the greatest risks are to our people in the field.

1.4 Our Health & Safety performance has improved significantly in the past 5 years and we have a rolling 3-year plan to drive health and safety compliance and year on year risk reduction, targeting a reduction in four key safety metrics: accidents; lost time accidents; days lost; and personal injury claims.

Questions this paper addresses:

2.1 What is the safety performance?

2.2 What are we doing to mitigate the key risks, including driving and robberies?

2.3 Are there any significant emerging risks?

Conclusion:

1. Performance continues to remain strong for all four of the key **health and safety metrics**, including absence accidents and lost days.
2. Mitigating action has reduced **road risk** which remains at a low level. Robberies have increased this year after an unusually low level in 2015-16. A number of additional activities are underway.
3. Additional **training workshops** have been planned for January to March 2017 for Persons in Charge of Crown Offices to enhance understanding of responsibilities and improve compliance.
4. Following the restructure of the GE and direct reports, individual 'deep dive' H&S sessions will be rearranged from January 2017.
5. The optimal balance of reporting and oversight will be re-considered over Q4, taking into account the Board, ARC, GE and the Safety Committee.

Input Sought

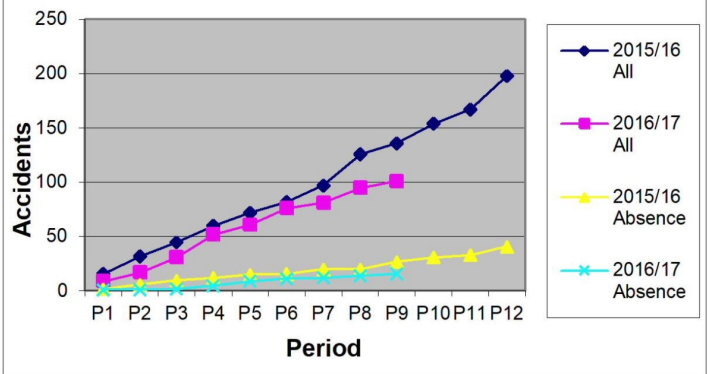
The ARC is requested to **note** the update on safety.

POL00247018

The Report – H&S Metrics

Summary of Safety Performance - YTD Period 8/9 (Nov 2016/17)

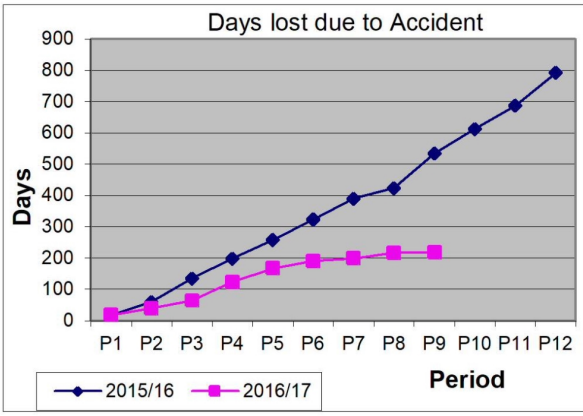
All Accidents – YTD Cumulative at Period 9
(Target to achieve a 5% year on year reduction)



Accidents have reduced 26% and **'lost time accidents'** 41% YTD by Period 9 (Dec 2016) v 15/16

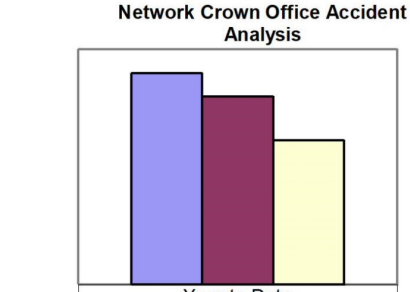
Lifting / Handling related accidents have reduced 50% over 2 years.
'Best practice H&S guidance' was included in our Christmas Arrangements and advice issued to Christmas Makers. Initial indications are a lower number of accidents reported for December.
Big improvement in 'lack of attention' related incidents reduced by 50% compared to 2015/16

Days lost due to Accident



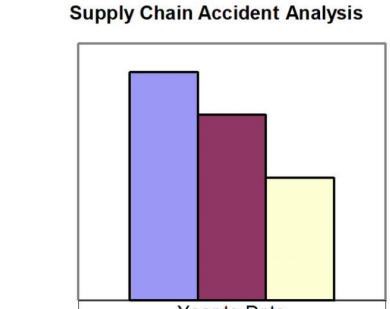
Crowns lost days P9 YTD : 45 (316 in 2015/16)
Supply Chain lost days P9 YTD : 174 (470 in 2015/16)
Support lost days P9 YTD : 0 (6 in 2015/16)
Trauma absence days– Supply Chain P9 YTD: 137 (296-15/16)

Crown Office Accidents YTD P8



	Year to Date
14/15	63
15/16	56
16/17	43

Supply Chain Accidents YTD P8



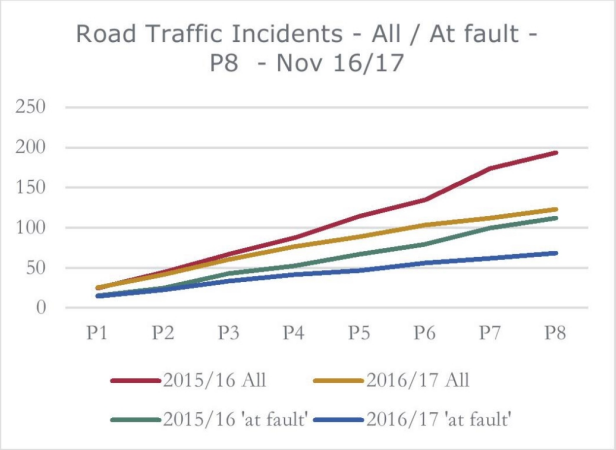
	Year to Date
14/15	80.0
15/16	65.0
16/17	43.0

Lost Time Injury Frequency Rate (LTIFR)

Supply Chain
YTD P9 – 0.740
2015/16 out turn – 1.042
2016/17 target – 0.990

All Post Office – Employee
YTD P9 – 0.216
2015/16 out turn – 0.370
2016/17 target – 0.350
PO Benchmark – 0.480

POL00247018



Current road risk performance has improved by 37% compared to P8 2015/16.

'At fault' incidents are also down by 39% P8 YTD (Nov).

Currently working through a tender evaluation for the provision of Commercial Fleet and Company Cars, accident management and maintenance. We expect better MI and analysis. Mobile Phone Policy communicated. A new compliance training module will be issued to capture a record.

Post Office CViT Robberies – P8 (Nov 16)
There have been 18 incidents reported in 2016/17 compared to 4 in 2015/16 which was an exceptionally strong year, however, this is a reduction on numbers reported in 13/14 and 14/15.

Post Office (All branch types) Robberies – P8 (Nov 16)
There were 18 incidents reported in November compared to 12 in 15/16 leading to some concern. A review is being undertaken and a response prepared for GE in January 2017.

The Report

2.1 What is going well across safety and what are the current activities?
2.2 What are we doing to mitigate the key risks, including driving and robberies?

SAFETY - Performance continues to remain strong for all of the key health and safety metrics, including absence accidents and lost days. Current activities include:

1. **Person in Charge (PIC) Training**

- Refresher Person in Charge training has been undertaken by all Supply Chain and Directly Managed Office managers with additional training planned for Jan-Mar 2017.
- Directly Managed and Supply Chain Lead Teams will also undertake the training.

2. **Property related risk**

- Overall risk has reduced from high to medium and will be low by year end.
- All high and medium fire risk actions completed, with support from Property and H&S Teams. Property Audits highlight housekeeping improvement opportunities especially Site Log Books, to be focused on in the workshops planned.
- Asbestos and Water risk assessments are currently being undertaken by CBRE.

3. **Supply Chain H&S Audit Programme**

- It has been agreed that Supply Chain will continue to operate to OHSAS 18001 H&S British Standard, externally audited. H&S Business Partners have audited Units in November and scheduled a number of additional audits in Q4 to ensure PIC training, documentation and procedures are compliant.

POL00247018

4. **Health & Safety Activity Calendars**
   To ensure Health & Safety activities are undertaken, relevant calendars have been updated and will be launched between January and March.
5. **Road Risk**

- Winter Safety Bulletin has been issued by the Fleet Management Team.
- A tender evaluation is currently being undertaken for the future providers of accident management, maintenance and repair of commercial fleet and company car fleet with an expectation of improved management information and accident analysis.

6. **Security / Robbery Risk**

- An update was provided in the GE December H&S Report. A report is being developed by the Head of Security to support a GE discussion in February due to an increase in Post Office robberies in November 2016.

2.3 Are there any significant emerging risks for 2017?

1. **Compliance to Driving and Mobile Phone Policy**
   The policy has been communicated on the Intranet and H&S home pages. The GE H&S Sub Committee has approved development and launch of an online compliance training module for business drivers.

2. **Simplifying Supply Chain, Support OD, Crown Franchise Programmes**
   There is evidence that reorganisation involving redundancies and increased job insecurity raises the risk of accidents caused by distraction and stress.
   Health & Safety Business Partners are monitoring absence, accident trends and causation and working closely with lead teams to ensure the focus on safety is retained and wellbeing resources have been communicated and are accessible.

3. **Hosted Directly Managed branches**
   Recent escalation of facility, heating and environment related issues have been discussed with the WH Smith Director of Risk. 'Ways of working' for Post Office and WH Smith managers and H&S mangers have been agreed and joint guidance is being written for Post Office and Store managers, and for colleagues working with Financial Service 'Pods and Cells'. Guidance should be issued by early February.

4. **Trauma Support and Suicide Policies**
   Additional training is being developed for call handlers in Chesterfield and the HR Service Centre to help them manage 'difficult calls' including threats of suicide. The training will be delivered from 23rd February. An external adviser is also reviewing a Suicide Policy for further consideration by Post Office.

5. **Security and lone working in Support Centres**
   H&S, Property and Security Managers are reviewing the security arrangements in place in all Support centres and satellite locations. A report will be developed for discussion by the H&S Sub Committee in March 2017.

POL00247018

Risk Update

Author: Jenny Ellwood Sponsor: David Hussey Meeting date: 20 January 2017

Executive Summary

Context

In November 2016 the Audit and Risk Committee (ARC) were provided with an overview of the management of Transformation risks. The paper described how risks were managed and gave a high level analysis of the Transformation risk profile, how the portfolio was performing and the key challenges being faced.

This paper builds upon that earlier narrative by looking in greater detail at the risk profile with particular focus on risk types (including changes to the profile), churn rates and risk weightings. It also provides analysis of overall trends to give a picture on how it is expected that the risks (in terms of number and weighting) will change both in their current and forecast status. It is inevitable such projections have a degree of uncertainty. Therefore a range of measures are already being put in place (such as risk appetite metrics, in-flight reviews and the implementation of a Post Office wide change policy) to manage this within acceptable tolerance.

Questions addressed in this report

- What are the top risks currently being managed within the Portfolio and what is the performance of risk management based on the mitigation plans?
- What are the types of portfolio risks and how has this mix changed?
- What is the current churn rate of portfolio risks?
- What is the current risk weighting of the portfolio and how is this expected to change?

Conclusion

1. The top risks within the Portfolio are i) Resourcing – Off Payroll Legislation, ii) IT Delivery capability and iii) Complex Change Portfolio Delivery. The Off Payroll legislation comes into force in April 2017, and the industry are still working through the implications. However, Deloittes are supporting the Post Office with the requirements. IT Delivery capability is reducing in terms of the impact and probability as mitigating actions are delivered and there are strong mitigation plans underway to manage the complex change portfolio.

2. There are currently 35 risks managed at Portfolio level, which Transformation consider consistent with the nature and complexity of the individual projects and the timeline. There are no major changes to the mix and there are currently no critical risks identified. 18 are considered significant (51%) and 17 are rated major (49%).

3. There is a regular churn of risks within the Portfolio. However, the overall number of active portfolio risks at the end of each month has been broadly

POL00247018

consistent over the last 12 months. The current residual risk exposure continues to track to be within the Transformation risk appetite and threshold.

4. The risk weighting has slightly increased. Paragraph 16 shows the risk weighting over the last eleven months, this weighting is calculated by multiplying their impact/probability scores. When added together this provides a cumulative portfolio score. Whilst this is quite a simplistic view it does allow comparison over time and tracks the movement of the risks within the Portfolio.

Input Sought

The ARC are asked to note the progress made since the last ARC, the top risks being faced, how they are being managed and mitigated and to advise on any additional areas/topics that should also be taken forward.

POL00247018

The Report

What are the top risks currently being managed within the Portfolio?

1. As at 5 January 2017, there are 35 open risks being managed at a Portfolio level. The 3 top risks, which have previously been reported to RCC and ARC, are:

   i) Resourcing – Off Payroll Legislation
   ii) IT Delivery Capability
   iii) Complex Change Portfolio Delivery

2. The new Off Payroll legislation comes into force in April 2017. The industry is currently working through the implications and full requirements. Transformation are working with Deloitte and Legal to understand the POL impacts. It is expected Transformation delivery costs will increase and, whilst increased funding will help reduce the impact of this risk, the Post Office may be unable to retain/attract the required resourcing through this mitigation.

Risk Title	Risk	Current RAG	Mitigation Plan	Due date	Target RAG
(i) Resourcing – Off Payroll Legislation	There is a risk that HMRC legislative changes effective from April 17 cause significant impact to Transformations current resource model.	**15** **I/P** **3:5**	• Obtain appropriate legal / tax expert advice **(in progress)** • Run contractor scenarios through the HMRC guidance and confirm tax liability for templated and specialised roles **(in progress)** • Work with Business Leads to run through contractor resource and their criticality to the Programmes and develop action plan / contingency approach **(in progress)** • Establish level of assurance POL need to complete where POL obtain resource through a third party supplier **(in progress)** • Reforecast change demand to identify required resource and skill requirements for 2017/2018 **(in progress)** • Develop comms plan for GE/Exec **(in progress)** • HR to confirm the preferred mix of change resource in terms of perm to contractor **(in progress)**	Mar 2017	**12** **I/P** **3:4**

3. The impact and probability of the IT Delivery Capability risk is reducing. Four new interim roles are in place and IT delivery is under tighter control. Recruitment is underway for permanent resource to fill these roles. IT System infrastructure and Data Centre refresh reviews are underway. Networks and Branch Technology reviews are complete. Work continues to improve the overall IT change process. Key pressure points are now immediately tackled with longer term resolutions piloted. There remains a costs/benefits risk with the historical IT projects.

POL00247018

Risk Title	Risk	Current RAG	Mitigation Plan	Due date	Target RAG
(ii) IT Delivery Capability	There is a risk that Transformation cannot be delivered in line with costs and benefit due to weak POL technical leadership capability, continuity of key people and IT Change Programmes designed for high risk single implementations	**16** **I/P** **4:4**	• Review the 1st phase of the IT Change Process and deliver quick win changes **(Complete)** • POL to increase IT in-house capabilities **(in progress)** • Review the next phase of change delivery to identify improvements and efficiencies **(in progress)** • IT to review system infrastructure **(in progress)** • IT to agree new ways of working with vendors **(ongoing – continuous improvement process)**	Mar 2017	**6** **I/P** **3:2**

4. There are emerging pressure points within the change portfolio with the first arising between March and June 2017 within field support and whether there is sufficient capability to manage the proposed changes. The integrated plan is key to the identification of hotspots and conflicts as decisions can be made on how these are managed and the impact they may have on benefits delivery.

Risk Title	Risk	Current RAG	Mitigation Plan	Due date	Target RAG
(iii) Complex change portfolio delivery	The next phase of Transformation will have increased dependencies and interconnectivities leading to more complexity to manage, which if not managed well could significantly impact our execution plans.	**16** **I/P** **4:4**	• Develop a single Business and IT Master Plan to schedule and smooth Change Delivery **(in progress)** • Create a single view of Change **(in progress)** • Ensure clear lines of accountability between Change Programmes and Enterprise Portfolio Management **(in progress)** • Produce new integrated plan and identify scheduling and hotspot constraints **(in progress)**	Feb 2017	**12** **I/P** **3:4**

5. In addition to the risks above there were three additional risks reported at November's ARC. These are being closely monitored, some of which have reduced in terms of impact and probability. These are:

   i) IT Vendor Renegotiations
   ii) IT Supply Chain Management
   iii) Capacity of IT Suppliers

6. Negotiations with IT Vendors are underway and remain difficult. There is however, increasing confidence with the majority of vendors and that the risks here, if realised, are more operational than change delivery. The main change delivery risk is around the Fujitsu renegotiations. If POL cannot renegotiate as planned this may impact the Network Development Strategy delivery timeline particularly around thin client development and cloud migration. This would also create further operational risks within the POL branch network.

POL00247018

Risk Title	Risk	Current RAG	Mitigation Plan	Due date	Target RAG
(i) IT Vendor Renegotiations	There is a risk that IT Vendors engagement is proves difficult and they display poor behaviours through renegotiations which could impact successful change delivery	**16** **I/P** **4:4**	• Establish Legal support for contract renegotiations **(in progress)** • Hire negotiation and procurement expertise **(in progress)** • Contract Managers are in place to manage transition and ensure Vendor SLAs and commitment is maintained **(in progress)** • Leverage GE/Board and other connections **(in progress)**	Feb 2017	**9** **I/P** **3:3**

7. The IT Supply Chain Management risk is being closely managed by IT. There is increasing confidence around this because IT have been working with key suppliers to introduce new ways of agile working. They have been supportive to the new approach. Work continues on improving the end-to-end change management process and the benefits of the new recruits within IT are being realised.

Risk Title	Risk	Current RAG	Mitigation Plan	Due date	Target RAG
(ii) IT Supply Chain Management	There is a risk that change is not managed effectively and efficiently due to: 1) the change delivery model and the ATOS SIAM operating model which adds complexity and overheads and; 2) the inability of POL to effectively manage suppliers from both a technical and leadership perspective	**12** **I/P** **4:3**	• Move the IT Change Operating Model from traditional 'Waterfall' IT delivery to 'Agile' methods **(in progress)** • Review/redesign E2E IT Change Management process **(in progress)** • Hire the right people with the right experience and capability and create persistent teams **(in progress)** • Reduce Project Manager overhead through the supply chain **(in progress)** • Create different ways of working with Suppliers to ensure projects & programmes adopt Agile risk reduction methods **(in progress)** • Develop a BAU contract management methodology **(in progress)**	Mar 2017	**8** **I/P** **4:2**

8. The risk related to the capacity of key IT Suppliers is also under close supervision and whilst IT are currently comfortable with its management, there are number of Transformation Programmes flagging that Fujitsu capacity is a risk to their Programme deliveries (i.e. Enhanced User Management and Transaction Simplification). The IT Vendor Management team has been strengthened, regular face to face reviews are in train and clear escalation routes developed.

Risk Title	Risk	Current RAG	Mitigation Plan	Due date	Target RAG
(iii) Capacity of Key IT Suppliers	There is a risk that key IT suppliers cannot meet our change demands due to pace of change and activity concurrency	**12** **I/P** **4:3**	• Secure persistent delivery teams aligned to strategic goals and purpose of POL **(in progress)** • Continue Vendors monthly reviews **(in progress)**	Ongoing	**8** **I/P** **4:2**

POL00247018

Risk Title	Risk	Current RAG	Mitigation Plan	Due date	Target RAG
	resulting in delays to delivery plans		• Contract Managers to monitor vendor capacity and delivery and escalate issues to TDG and GE **(in progress)**		

9. A full list of the 35 portfolio risks is shown as an Appendix

What are the types of portfolio risks and how has this mix changed over time?

10. At the last ARC meeting in November 2016 there were 33 portfolio level risks. There is a regular churn of risks at portfolio level. Since the last ARC Transformation has seen a net increase in the number of open portfolio risks which now stand at 35. Figure 1 below illustrates how the mix of risks at portfolio level has flexed in recent weeks. Noting that green risks are managed at a local level and not escalated to Portfolio view.

RAG Impact/Likelihood	Minor (1)	Moderate (2-4)	Major (5-11)	Significant (12-19)	Critical (20-25)	Total
Current Month	0	0	17	18	0	35
Previous Month	0	0	14	18	1	33
% of total (current period)	0%	0%	49%	51%	0%	100%

Figure 1: Open portfolio risks by severity (October and November 2016). Please note the minor/moderate risks are managed at a local level and not escalated to the Portfolio view.

11. The current risk mix is broadly comparable with what Transformation faced back in June 2016. With risks relating to finance, IT and resourcing being the highest concentration. As new tranches of work materialise it is expected the number of risks will increase at Programme level and also fluctuate at Portfolio level.

12. Additionally, the POL cost reduction plans over the next 3 years will need to be carefully managed as they may increase the current people risks in relation to loss of key capabilities and corporate memory (knowledge and expertise) resulting in errors and increased resourcing costs.

What is the current churn rate of portfolio risks and what are future projections?

13. The overall number of active portfolio risks at the end of each month has been broadly consistent over the last 12 months. In November 2015 Transformation were managing 42 portfolio risks which peaked at 59 the following month. Since then there has been a gradual reduction, month on month, to bring the number of open portfolio risks, at any one point, to around 30.

14. Figure 2 below details the number of risks open and closed over the last 6 months. It illustrates the degree of churn at portfolio level and provides evidence of the proactive management of risks at this level.

POL00247018

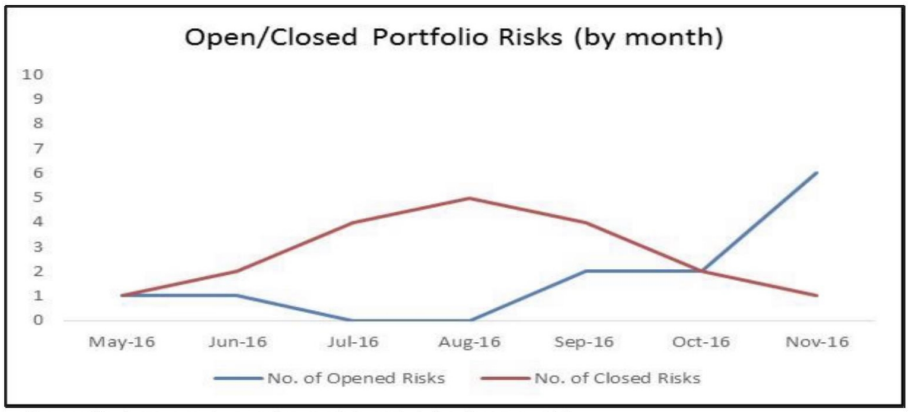


Figure 2: A comparison of open/closed risks (by month)

15. Transformation consider the current number is reflective of its overall objectives, the nature of the individual projects and the timeline it is committed to over the next 18 months.

What is the current risk weighting of the current portfolio and how is this expected to change over time?

16. Each risk has a weighting score calculated by multiplying their impact/probability scores. When added together this provides a cumulative portfolio score.

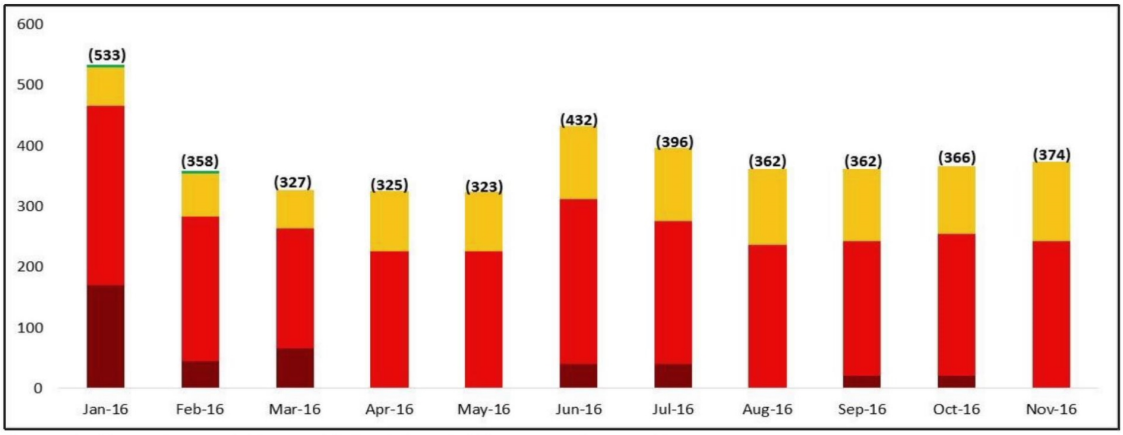


Figure 3: Current cumulative portfolio risk weighting score by month

17. Confidence remains high that the portfolio remains broadly on target and that the associated risks (albeit many of which have relatively high risk weightings) has shown a degree of stability in recent months.

POL00247018

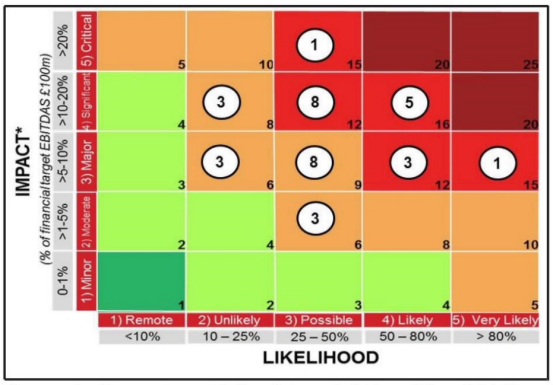


Figure 4: Current portfolio risk weighting (Nov 2016)

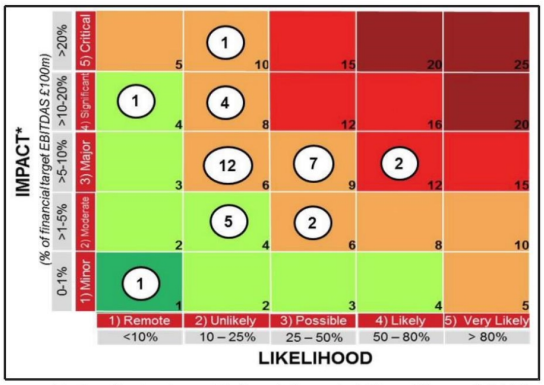


Figure 5: Projected portfolio risk weighting (June 2017)

18. Figures 4 and 5 illustrate the anticipated impact of a reduction in the number of active risks (within the current portfolio) over the next 6 months will have on the residual risk weighting. In part this is because a significant number of the current portfolio risks will reach their target risk weight (which will be in line with risk appetite). This does not taken into account, of course, the impact that newly identified risks will have on the portfolio.

POL00247018

Appendix: Transformation Portfolio

Top Risks

	Risk Title	Grid Ranking CURRENT	Grids Ranking TARGET
1	IT Networks Branch and Admin Delivery Risk	16	6
2	IT Vendor Renegotiations	16	9
3	Complex Portfolio Planning & IT Management *	16	12
4	Transformation Delivery oversubscribed	16	9
5	Business Process Management	16	9
6	IT Delivery Capability *	16	6
7	Resourcing Risk - Payroll Legislation *	15	12
8	IT Networks Branch incumbent supplier proactive engagement	15	10
9	IT Supply Chain	12	8
10	Branch Technology Business Case	12	8
11	STRN ePOS Solution Uncertainty	12	6
12	Financial risk - Insufficient Funds to deliver Transformation	12	9
13	IT Strategy - Alignment with Transformation	12	9
14	Delivery - Integrated Plan Delivery Performance	12	6
15	Capacity of IT Key Suppliers	12	8
16	Data Management Strategy	12	9
17	Supply Chain Risk	12	6
18	Data Quality	12	9
19	Portfolio Plan	9	6

POL00247018

	Risk Title	Grid Ranking CURRENT	Grids Ranking TARGET
20	Unintended consequences on Operational Performance – Process	9	6
21	Availability of Key Skills and Knowledge	9	6
22	Unintended consequences on Operational Performance – People	9	6
23	Responsible use of public funds	9	1
24	Change Fatigue	9	6
25	Cost of VR	9	6
26	Siloed Working Practices	9	6
27	Financial risk - Benefits/Revenue Realisation	8	6
28	Deployment of Non-Compliant Solutions/Systems - (Breach of LRC requirements)	8	4
29	Reputational Damage - Political stakeholder risk (national government)	8	8
30	Strategy & Design: Conflict between current BaU and Transformation activities	6	6
31	Accounting & Reconciliation	6	4
32	Cost Reduction Initiatives impact Transformation requirements	6	4
33	Reputational Damage - Media risk	6	4
34	Poor coordination of communications about change activity with stakeholders and employees	6	4
35	Reputational Damage - Political stakeholder risk (local government)	6	4

* Risks that were reported to RCC/ARC in November 2016

POL00247018

Criminal Cyber Attack on Post Office Telecommunications Business

Author: Geoff Smyth Sponsor: N Kennett/R Houghton Meeting date: 11.01.2017

Executive Summary

1. The Post Office Telecoms business is run in close partnership with Fujitsu who are responsible for managing the full supply chain, including Talk Talk (Network) and Zyzel (Router manufacturer). Fujitsu are responsible for operations and technology, while Post Office retains control of strategy, marketing, pricing and trading.
2. During the weekend of November 27/28, a global cyber-attack was launched with the apparent aim of recruiting vulnerable telecoms consumer routers for a large scale DDOS attack on as yet unnamed targets. In the industry this is known as a "BOT" attack.
3. It is believed that all Telecom's providers were targeted but only those with certain brands of routers were compromised, over 50 service providers in the UK were directly impacted.
4. The vulnerability exploited by the hackers was an open port in the software used to remotely manage the router estate and diagnose faults. This software is known as TR69, and the exploited port was in a complementary LAN software platform TR64. The software collectively forms part of the routers firmware.
5. Post Office has a customer base of 200,000 routers, of which 135,000 were vulnerable and were consequently compromised.
6. The impact of the attack, however appears to have been unexpected. A router once infected began to initiate a re-authentication request to the Fujitsu Automated Configuration Server (ACS). This request was constantly repeated causing the router to attempt to persistently re-register. The net effect was either to disable or slow the customer's access to the internet.
7. The attack on Post Office began at some time on Sunday November 28 and by Monday Fujitsu had identified unusual network traffic volume and the call centre was experiencing an 800 % increase in expected call volume. Fujitsu escalated the issue to Talk Talk in Warrington, and work began on diagnosis.

POL00247018

Questions addressed in this report

1. What happened?
2. What are the consequences for the business?
3. What preventative measures have been put in place to stop this happening again?
4. Did the Post Office handle this incident effectively?
5. Could the incident have been avoided?
6. Who is accountable for incidents of this nature in the future?

Conclusion

7. The Post Office responded quickly and effectively, and in particular Fujitsu our managed services partner provided the leadership, insight and resources to co-ordinate the response.
8. Post Office was the first UK ISP to develop and deploy a software patch that inoculated customer's routers, and provided the mechanism to purge the infection.
9. Talk Talk also performed well during the initial diagnosis and deployment phase, however swifter action on their part following Fujitsu's request to close the network port has identified an opportunity to tighten their escalation process.
10. The attack was unexpected, both for the Post Office and the industry. No industry body (as far as we are aware) had considered that customer routers were a possible BOT attack platform.
11. No customer data or customer owned devices were compromised as a result of the attack.

POL00247018

The Report

What happened and how did the business respond?

1. An industry-wide vulnerability within the operating system of the vulnerable routers was exploited by the hacker (s) using a variant of the Mirai worm. The Mirai worm is Malware (virus) that is designed to recruit the infected device so that it can be controlled remotely to launch a DDOS attack on another third party website. DDoS is short for Distributed Denial of Service. DDOS is a type of attack where multiple compromised systems, which are often infected with Malware, and are then used to target a single system causing a Denial of Service.
   The motives of the hackers using the Mirai worm to-date has been the DDOS attack of high-profile services. As a result we have concluded that the likely motive was a botched attempt to recruit customer routers to a larger BOTNET for a future attack on another company.
2. 135,000 customers were potentially vulnerable to the attack, of which 108,000 were actually infected with Malware.
3. The extent and detail of the attack was determined by 10 pm on Monday November 28th. The diagnosis was assisted by the online publication of a news report that Deustche Telekom had suffered a cyber-attack impacting 900k of their customer's routers.
4. The router manufacturer Zyxel was contacted and supplied with the information. They immediately started to work on a patch for the vulnerability which had been discovered in the TR69/64 stack of the operating system of the router.
5. Investigations discovered that the vulnerability was exploiting network Port 7547. A request was made into TalkTalk close that port at a network level. At this juncture it appeared that the problem was isolated to the Post Office as no other UK ISP had either recognised or reported a problem, as a result Talk Talk did not close the port.
6. On Tuesday 29th Nov 14:00 the software patch and deployment method created in partnership between Zyxel and Fujitsu had been tested and delivery to the router estate commenced. In addition ACS server capacity was upgraded by Fujitsu to cope with the additional demand.
7. On Wednesday 30th Nov, 40k routers patched within the first 24 hours and Talk Talk continue to investigate the impact of closing port 7547. At 22:00 TT informed Fujitsu that they have made an Executive decision to close port 7547. The change of direction was attributed to their reassessment of the threat level to all their network customers.
8. By Friday 2nd Dec, 80% of the routers visible to the ACS had received the patch, and were declared infection free. This was also supported by the fact that call volumes had dropped significantly.

POL00247018

9. The contact centre opening hours were extended until 11 pm, and unlimited overtime was offered to all agents. This prevented an unmanageable volume of work-flow queues being carried over into the following week.
10. Over 60% of the calls were related to reconnecting WiFi devices and not specifically about rebooting the router. This suggests that the majority of customers were able to deal with the initial infection, but then required help to restore their home network devices.
11. On Monday 5th Dec Fujitsu resumed the mopping up of the tail of infected routers.
12. On Tuesday 6th Dec TalkTalk contacted Fujitsu highlighting that they could see a number of our routers continuing to create high levels of traffic attempting to contact 3rd party hosts on the internet, these attempts were being blocked.
13. Fujitsu's remote monitoring software identified 15k of router estate as still requiring rebooting to clear the Mirai worm present in the router.
14. On Wednesday 7th Dec, an outbound automated calling program was launched to contact the remaining 15k customers, with instructions to reboot their routers. The initiative began to show an immediate impact with 1700 routers purged within the first hour, and re-connected to the ACS.
15. Less than 200 routers remain uncontactable, the majority of these are customer sourced routers (purchased), and thus unlikely to be infected. However in order to fully satisfy ourselves that the infection had been fully purged, these users have been placed into a "walled garden" and when they next connect to the internet, they will be directed to either a web page or the contact centre to conduct a reboot of the router.

What were the consequences for the business?

16. 108,000 customers were either denied access to the internet, or had their speed impacted for between 3 and 6 days.
17. At this juncture we have not seen a spike in churn however it is possible we will lose a few customers as a result. Anecdotal feedback from our contact centre agents indicate that customers did recognise that this was a criminal attack, and that their personal data was safe.
18. The costs of increased call centre hours and the outbound call campaign is estimated at £140,000. Only 338 customers requested credits for a total of £1500.
19. In summary the most material impact was to customer experience, however the vast majority of customers have been understanding and we have not yet seen an increase in customer churn.

What preventative measures have been put in place to stop this happening again?

20. At a network level TalkTalk have blocked port 7547 to prevent further attacks infecting their network, and our routers.

POL00247018

21. On the router the TR69 vulnerability has been closed.
22. A further non-intrusive patch will be deployed which addresses the TR64 port and renders it completely closed.
23. There are no changes contemplated within the Fujitsu network operations centre in Solihull as after review their level of monitoring was effective and timely.
24. Consideration is being given as to whether the Post Office or Fujitsu should invest in a customised internet monitoring service (including the Dark Net) to alert us to future threats before attacks are launched.

Did Post Office handle this incident effectively?

25. Yes. Post Office via our managed services partner Fujitsu were the first ISP in the UK to recognise that we had been the victim of a criminal cyber-attack on our network.
26. Once the attack was confirmed the Post Office team comprising Fujitsu, Talk Talk and Zyzel swiftly developed, tested and deployed a router software patch. This required working round the clock during the first 24 hours.
27. The initial PR statement issued at 1.30 pm on Thursday December 1st as a response to a BBC enquiry emphasised that no personal data or any personal device was compromised. This statement allayed many customers' fears of the impact of the attack. In hindsight Post Office may have been able to communicate more effectively with our customers had we adopted a proactive PR strategy and briefed the media late on Tuesday November 29th. However when the story did break on Thursday December 1st, the reactive statement was clear and concise.
28. The story was published by the BBC online news at 3.30 pm with Post Office as the lead company impacted, but by 5.30 the headline was Talk Talk and Post Office, as a result Talk Talk dominated the headlines.
29. The call centre was severely impacted with extremely high call volumes exceeding 600% over the initial few days, and consistently running at 150% in the second week. In order to mitigate the impact on customers operating hours were extended, and unlimited overtime authorised. In the circumstances this was the most effective response, as deploying untrained agents for this type of attack was not practical or prudent.
30. Internal stakeholders were kept informed via the ATOS incident reporting process. The Director of Telecoms also kept the GE informed via email updates.

Could the Incident have been avoided?

31. The instructions for how to modify the Mirai worm code to enable it to attack customer routers was published on the "Dark Net" on November 7, 2016. It does not appear that router manufacturers/network operators, where relevant, noted the publication of the instructions and as a result the industry was unprepared for this unique attack. A systematic monitoring of threats to residential telephony networks may have identified the modification of the Mirai worm for a BOT attack.

POL00247018

32. In addition one of Post Office's customers, Ross McKelvie did alert our customer service centre via email in October 2015 of his concerns that the router port 7547 (which is used for remote management and support via TR069) was open to the internet.

In summary the customer email raised four key concerns as follows:

Issue	Agent fact finding	Agent action
TR69 platform has a vulnerability to the "Misfortune" cookie	Vulnerability had been previously identified and fixed in a firmware update in Jan 2015	Acknowledged but not communicated to the customer, file notes indicated "closed"
Pc World article highlighting mass router vulnerability	Article was found to be factually incorrect	Acknowledged but not communicated to the customer, file notes indicated "closed"
Router is open to the internet	The Router is not open to the internet as upon shipping it can only communicate with the ACS server and thus is not initially vulnerable to any internet threats	Acknowledged but not communicated to the customer, file notes indicated "closed"
7547 Port requires blocking at the network level	7547 is open on the router to enable remote management via TR069 as designed and would therefore not be practical to disable on the device.	Acknowledged but not communicated to the customer, file notes indicated "closed"

Based on the specific issues raised and the agent investigation, the ticket was closed by the agent without escalation. While the agent did perform the task assigned given the nature of this email the matter should have been escalated to second line technical support for resolution. However in this instance the frontline agent conducted the investigation and closed the ticket.

In reviewing the HGS agent performance the following is relevant:

- HGS had only recently begun Technical support services replacing Capita
- The agent had been in a front-line role for 2 days
- The agent failed their probation following 90 days and was released by HGS

33. The customer did identify himself as a security expert, from Norbroch Consulting, and is the founder. In subsequent emails in the last month he does acknowledge that he should have made more effort to escalate to senior leadership, or follow-up with customer service.

POL00247018

34. In reviewing this case had the email been escalated to a management level it is not clear if a different conclusion would have been reached. The attack in November 2016 was conducted in a manner not consistent with Mr McKelvie's hypothesis. Furthermore it was not envisaged by any of the relevant parties; Fujitsu, Talk Talk, Zyxel, or as far as we are aware, by any other industry body or service provider. To make a change of the type and scale required, the threat would have to be well documented and tangible. Neither condition existed at the time.
35. In summary the benefit of hindsight suggests that if a certain line of escalation had been followed then it is possible that the specific router vulnerability would have been detected by Talk Talk who in turn would then have closed Port 7547 at the Network level. This would have prevented the infection of all vulnerable routers on the Talk Talk network. This is however speculation, and the lack of any follow up by the customer as a security expert ensured that no further action was taken.

Who is accountable for incidents of this nature in the future?

36. At present the accountability rests with the Director of Telecommunications reporting to the GE member responsible for the function, in this case Chief Executive Financial Services and Telecommunications, Nick Kennett. However as this incident was a cyber-attack, it has highlighted the fact that cyber security is the responsibility of the Group CTO, Rob Houghton. Further this incident impacted customer premise equipment which has not previously been considered part of the Group CTO's responsibility.
37. The technology platform (s) supporting the Telecommunications business have been developed by and fully outsourced to Fujitsu. The technology platform(s) are an integral component of the delivery of Post Office's telecommunications service to 480,000 customers. The contract with Fujitsu is an extensive and comprehensive, and contains specific data security provisions. However there are no specific cyber security accountabilities specified. As a consequence there are no cyber security flow-down clauses to other suppliers.
38. In summary the current accountability rests with the Director of Telecommunications but this should be reviewed and either confirmed or amended as necessary. Further consideration should also be given to developing standard cyber security provisions for all relevant Post Office contracts that any potentially impacted by cyber security threats.
39. Investment in cyber threat monitoring should be seriously considered.

POL00247018

5.1) Annual Risk Review: Financial Crime

Author: Sally Smith Sponsor: Jane MacLeod Meeting date: 30th January 2017

Executive Summary

Context

The Terms of Reference of the Board Audit & Risk Committee include oversight of management of financial crime within Post Office. These include Fraud, Anti Bribery and Corruption and Anti-Money Laundering and Counter Terrorist Financing. Further the suite of policies approved during 2016 anticipates an annual review of the effectiveness of those policies. This paper provides the Committee with an update on the key Financial Crime risks identified, their performance and what this means for our control environment.

Questions this paper addresses

- **What are the key risks?** *which risks are outside of our risk appetite/ causing concern? What are the key metrics? How are these risks performing? Have there been significant incidents or exceptions?*
- **Governance and assurance:** *what governance mechanisms are in place? Where does assurance come from? Have issues been identified with the control environment?*
- **Overall assessment:** *how does this impact our key decisions? What should we stop doing/ start doing/ do differently?*
- **Further actions:** *what further actions are being taken? What are the next steps?*

Conclusion

1. The key Financial Crime risks for Post Office relate to the effectiveness of the control environment to limit activities undertaken by third parties through Post Office that support anti-money laundering and terrorist financing, as well as fraudulent activities undertaken by third parties against Post Office or by agents themselves.
2. While the majority of these risks are deemed to be of moderate or low risk, very few are within the currently applicable Board approved 'averse' risk appetite for:
    - financial crime to occur within any part of the organisation; or
    - not complying with law or regulations or deviating from business conduct standards.
3. The highest area of risk for Post Office is AML/CTF for which we are directly regulated by HMRC. AML/CTF risks are the subject of a separate annual report by the Post Office MLRO. Significant work will be required during 2017 to address the

POL00247018

concerns identified in that report and to develop pro-active (as opposed to reactive) controls.

4. Assessment of threat levels is restricted due to a lack of data and MI, and current under-resourcing. There are general risks to Post Office in terms of loss through fraud due to poor systems architecture which limits fraud prevention, and insufficient data capability to enable early detection. A number of recent frauds have highlighted system weaknesses that could be more widely exploited. Manual mitigating controls have been put in place for a number of these, including prioritisation of the reconciliation and settlement processes which facilitate earlier identification of frauds.

5. There has been significant assurance activity in relation to Post Office's Financial Crime capability and compliance over the last 12 months including external reports from Promontory, risk assessments by Thistle Initiatives and the current HMRC audit. In addition, the internal governance framework has been enhanced with the establishment of the Fraud, Loss and Crime Forum under the chairmanship of the CFO. Regular reports have also been provided to both the Risk & Compliance Committee and the ARC on financial crime issues.

6. At the time of writing, work is still underway to finalise the risk assessment in relation to Anti-Bribery and Corruption compliance within Post Office, however initial findings suggest that this is an area of lower concern for Post Office than AML/CTF. A verbal update will be provided to the Committee on the conclusions from this risk assessment.

7. Findings from the HMRC audit into AML/CTF controls were due to be delivered during January 2017 but are now not expected before the ARC meeting. These, together with outcomes of the anti-bribery review, and product specific AML risk assessment work, will result in the development of an action plan to address the findings. Progress against this plan will be regularly reported to the RCC and the ARC during 2017. Key areas to be addressed include increased resourcing, enhanced MI and systems capability, and continuation of the program of product risk assessments.

8. In response to these issues:
   - Resourcing in the financial crime team is being enhanced;
   - The Financial Crime team is reviewing systems enchancements that would support pro-active monitoring of risks, and the cost of these has been flagged through the Change portfolio; and
   - Product risk assessments are underway, and will continue on a risk weighted basis during the remainder of 2017.

Input Sought

The ARC is asked to review this report, endorse the recommendations and consider whether further actions should be considered.

POL00247018

The Report

What are the key risks? Which risks are outside of our risk appetite/ causing concern? What are the key metrics? How are these risks performing? Have there been significant incidents or exceptions?

9. The risk register maintained by the Financial Crime team currently identifies 60 separate risks relating to Financial Crime as follows:

   - Fraud –26 risks of which 16 are assessed as 'Amber' and 10 are 'Green'
   - ABC –8 risks of which 4 are assessed as 'Amber' and 4 are 'Green'
   - AML/CTF –26 risks of which 6 are assessed as 'Red' (details of which are set out in Annexure A), 15 are 'Amber' and 5 are 'Green'.

   Due to inadequacies of the available MI, it is not possible as yet to provide meaningful performance data in respect of these risks.

10. To date, issues have been identified in relation to the following products and processes:

    - non-conformance with Bureau de Change limits;
    - Mandatory and suspicious activity ID capture;
    - Insufficient regulatory transaction monitoring;
    - Suspicious Activity Reporting (SAR) failure; and
    - Due diligence for Bureau de Change business relationships.

    Further details are included in Appendix 2. The key risk arising from each of these is that Post Office may not meet its regulatory obligations, and there is therefore a risk of regulatory penalties. While HMRC does not at present publish details of regulatory penalties, this will change once the 4th Money Laundering Directive comes into effect later in 2017.

11. As part of their audit HMRC reviewed the bureau de change transactional data for 1,111 branches[1] and provided examples of potential non-conformance for Post Office to review, including:

    - two branches demonstrating unusual bureau activity; due to the limitations of the current manual monitoring processes, only one of these had previously been identified by Post Office ; and
    - transaction splitting in 92 branches. The transaction review undertaken by HMRC utilised specialist software with significantly enhanced capabilities to that currently available to Post Office. Our initial review of this data suggests that Post Office had already identified and investigated a number of these branches.

12. Discussions are underway with HMRC as to whether the cash processing previously undertaken by Supply Chain for MSB clients was within scope of 'Money Transmission' business and therefore regulated and subject to premises registration. While legal advice on this issue was taken, Post Office believes that

[1] approx. 10% as circa 10,452 branches involved in transacting Bureau de Change

POL00247018

HMRC's definition is unclear, and is in discussion with HMRC regarding this uncertainty.

13. HMRC previously advised that their audit report would be presented to Post Office during January 2017 however this has been further delayed due to resource issues within HMRC. In reviewing the issues that they have identified, HMRC will assess whether these amount to failures or actual breaches, the latter potentially being subject to regulatory penalty. We expect, at a minimum, a comprehensive action plan to address areas identified with strict delivery timescales. Failure to comply with these timescales will likely result in significant penalties being levied, although the potential amount is unknown.

14. We also expect to receive shortly a pre-penalty notice in respect of historic branch premises registration errors. Post Office have been advised verbally that 951 de-registration errors have been de-scoped from penalty, thereby significantly reducing the amount of the potential penalty. Whilst there has been no official guidance given, we now anticipate that the penalty will not exceed £500k . Post Office has now reviewed and enhanced the procedures and controls relating to branch registrations.

15. Post Office continues to participate in an information sharing agreement with the National Crime Agency, and the Head of Financial Crime regularly attends JMLIT meetings as a means of ensuring market intelligence and horizon scanning of issues relevant to Post Office activity can be considered on a pro-active basis.

Governance and assurance: *what governance mechanisms are in place? Where does assurance come from? Have issues been identified with the control environment?*

16. **Fraud:** There have been several large fraud losses in the last 12 months that have highlighted weaknesses in systems and processes (both back office and front line), and a new Fraud, Loss and Crime Forum was established in November to ensure appropriate operational oversight.

17. **Anti-Bribery:**Thistle Initiatives were commissioned to undertake a risk assessment of the ABC risks and controls within Post Office during 2016, and whilst this work is not yet complete, this work has not highlighted any additional significant risks.

18. **Money Laundering:** A number of reviews of the AML/CTF framework have been undertaken since 2015, both internally by the MLRO, and externally by each of Promontory and Thistle Initiatives. These have highlighted some significant risks for Post Office. Additionally there is the (external) HMRC audit, discussed above. Further details of these are set out in the MLRO report which is also included in the Committee papers.

19. Financial Crime risks are reviewed at the following:

    - Monthly Financial Crime Governance Meeting chaired by the MLRO – this forum reviews performance and issues at a granular level and provides governance and assurance to the MLRO that Financial Crime including AML, CTF and ABC regulatory requirements are being met. It also provides the MLRO with an overview of current investigations, interventions, non-conformance and regulatory issues relating to Financial Crime (fraud, AML, CTF and ABC) issues.
    - Monthly Fraud, Loss and Crime Forum, chaired by CFO - The overall objective of this forum is to ensure that the risk of Financial Crime loss is

POL00247018

managed effectively and proportionately across the business. The remit of this forum is to:

- Assess risks, audit results, issues and trends arising that may increase Financial Crime risk exposure.
- Review remediation plans, ensure that actions have ownership and that these are realistic, proportionate and deliverable.
- Monitor the progress of remediation plan implementation.
- Actively manage the cross-business response to resolution.
- Maintain oversight over current and emerging internal and external exposures that could result in loss or brand reputation damage.
- Review any material incidents affecting products and services which result in loss or regulatory impact.

20. New/updated policies for Financial Crime, AML/CTF and Anti-bribery were approved during 2016. Roll out of these policies to the business is ongoing. Assessment of the effectiveness of these policies will be undertaken in late 2017 and reported in the next Annual Review.

Overall assessment: *how does this impact our key decisions? What should we stop doing/ start doing/ do differently?*

21. There are a large number of risks relating to Financial Crime, however, most are deemed to be of moderate or low risk. There are general risks to Post Office in terms of loss through fraud due to poor systems architecture which limits fraud prevention and insufficient data capability to enable early detection. A number of recent frauds have highlighted system weaknesses that could be more widely exploited, however, mitigating controls have been put in place for a number of these, including ensuring that related reconciliation and settlement processes are given priority.

22. The highest area of risk for Post Office is AML/CTF for which we are directly regulated by HMRC. Historically, understanding around the controls required has been poor, with branch premises registration not being properly understood, nor kept up to date, and the regulatory requirements relating to Bureau de Change transaction limits, monitoring requirements and PEPs and Sanctions not being understood. Additionally, we are aware that the HMRC audit is likely to recommend that more data is captured at point of sale for Bureau de Change transactions and that transaction monitoring is improved.

23. Resource constraints driven by previous cost cutting measures as well as numerous changes of responsibility for fraud over the last few years have resulted in a lack of focus on compliance driven activities. As a result of the various assurance reports undertaken over the last 12 months there is now a greater appreciation of the regulatory obligations that need to be met in order for Post Office to continue to offer its current range of regulated products. Accordingly, in addition to the actions described below, further work will need to be done to develop a culture of compliance. This will involve enhanced and targeted training for customer facing and support roles.

24. The data and MI available to Post Office to understand both the current threat level and trends is poor. Data is received from Global Payments each month on the level of fraud reported on cards used in Post Office branches, and daily reports are received from Grapevine of any fraud or AML/CTF calls or incidents they have received, however we need to enhance the quality of the MI received and pro-actively managing these risks.

POL00247018

25. The range of work being undertaken through the various initiatives will allow us to consider whether Post Office should define its risk appetite on a more granular basis.

Further actions: *what further actions are being taken? What are the next steps?*

26. There are a number of actions which have been self-identified and which will need to be actioned in 2017. It is likely that HMRC will require various remedial actions to be undertaken arising from the current audit, however it is expected that these will, in many cases, align with those activities that have already been identified. In particular:

- Increased resourcing in the Financial Crime team will be required to enable Post Office to pro-actively identify and respond to financial crime threats;
- Enhanced systems and MI capability will need to be developed to facilitate the pro-active identification of suspicious trends and activity, which in turn will enhance controls over non-conformance and improve suspicious activity disclosure;
- Post Office will need to progress the product risk assessments using the methodology developed as part of the Thistle risk assessment. These assessments will be prioritised based on a combination of factors including the regulatory status of the products, contribution to revenue and profit, complexity, and known financial crime risks.

Mandatory training

27. Current monitoring of completion levels for mandatory training is manual and labour intensive, however with the full roll out of the Success Factors platform during 2017, these issues should be addressed. It was agreed by the November Risk & Compliance Committee that satisfactory completion of compulsory regulatory training will, going forward, be a gateway requirement for receipt of annual bonus. A communication to this effect will be issued early 2017 to coincide with the rollout of annual training.

Risk Assessment Mitigation Update

28. Thistle Initiatives are in the final stages of the pilot exercise for Bureau de Change. The pilot exercise will drive lessons to be learnt for future product risk re-assessment so whilst some early recommendations are specific to Bureau de Change, others should be considered more broadly in the context of Phase 2 of the overall Financial Crime Risk Assessment project. Preliminary findings are set out in Appendix 2.

29. Overall risk rating continues to indicate that Bureau de Change is one of Post Offices greatest financial crime exposures and the residual risk position is currently outwith Post Office current risk appetite.

Anti Bribery and Corruption Risk Assessment Mitigation Update

30. Thistle Initiatives were engaged to complete a detailed review of Anti-Bribery and Corruption (ABC) risks across Post Office. The assessment will report the potential inherent risks to Post Office and evaluate the strength of the mitigating controls in

POL00247018

place, ensuring a zero-tolerance policy to bribery is embedded within the culture of the business. The assessment has been designed to consider all business areas and third party relationships.

31. Thistle Initiatives issued 29 questionnaires across the business with 15 returned. Information has been gathered via telephone, face to face or email from 32 individuals and 101 plus documents have been received. There have been some issues with availability in some business areas, with approximately 8 individuals unable to participate. To date, there has not been any evidence of major failings within the ABC controls; a summary of the early findings is contained in Appendix 3. Information gathering was brought to a close on 20th January in order to draw a line and facilitate completion of the inherent and residual risk calculations. Submission of the Risk Assessment Matrix and accompanying Report is on schedule for the end of January.

32. The research carried out within the business has been concentrated on Finsbury Dials staff, specifically GE and senior management, as part of the assessment of 'tone from the top'. It is beyond the scope of this assessment to approach branch level staff directly.

33. Thistle will continue to collect further information until early January, when a cut-off date will be in place, the risk assessment completed and any recommendations made. The assessment will be created so it may continue to be utilised by Post Office, updated annually and reported to the board.

POL00247018

Appendix 1– Details of 'red' risks

1. Bureau de Change limit non-conformance:
    - To ensure Post Office adheres to the Money Laundering Regulations, bureau transactions are restricted to the equivalent of £10k per customer, cumulative over a 90 day period. Both the Promontory review at the end of 2015 and the recent risk assessment by Thistle Initiatives highlighted that there is a risk that staff are not adhering to these limits as the Horizon system does not prevent customers from exceeding the regulatory limit.
    - Current system limitations mean that it is very difficult to identify linked transactions (eg multiple transactions just under the £10k limit, multiple transactions by the same person within defined periods or in different branches), and Horizon is unable to restrict linked transactions. Controls currently in place (but which only partly address the above issues) include:
        - The Fraud Analysis team review any transactions of £5,000 and over and/or that are raised as suspicious by branches;
        - The Financial Crime team investigate referrals from stakeholders including the Fraud Analysis team and FRES and take appropriate action to mitigate.
        - Staff are reminded of the limits in annual training
    - As of December 2016, there were 14 branches on manual reduced thresholds as a result of serious non-conformance. HMRC have recently reviewed a subset of transactions over a 12 month period and have identified patterns that indicate higher levels of non-conformance. Due to poor access to data and manual monitoring processes, some these had not been identified by Post Office.
    - Current controls are only partially effective. Thistle Initiatives are completing a risk assessment of the bureau service which is due end of January 2017 and will highlight additional controls and data required to mitigate this risk.
2. Mandatory and suspicious activity ID capture:
    - Two forms of ID must be captured for any Bureau de Change transactions of £5k and above, or if the staff member is suspicious. ID details are frequently incorrectly captured on Horizon as the fields are free format and do not verify or validate the data format. This could be as a result of input error or deliberate to disguise linked transactions
    - There are not currently any systems in place to monitor or identify anomalies, however, the Fraud Analysis Team will review ID data as part of their over £5k transactions monitoring if there is a specific concern at a branch.
    - Current controls are ineffective. Thistle Initiatives are completing a risk assessment of the bureau service which is due end of January 2017 and will highlight additional controls and data required to mitigate this risk.
3. Insufficient regulatory transaction monitoring:
    - The Promontory review at the end of 2015 and the risk assessment by Thistle Initiatives in 2016 highlighted a number of concerns with Post Office monitoring systems and controls. Examples include:

POL00247018

- Heavy reliance on third parties to provide data
- The Horizon system does not enforce procedural controls relating to transaction limits at blanket and independent branch level
- Post Office has no screening software or fuzzy matching capability to robustly identify potentially linked transactions

- Currently monitoring can only be performed on transactions over £5k and this is a manual review conducted via excel spreadsheet and therefore has severe limitations.
- Current controls are ineffective. Thistle Initiatives are completing a risk assessment of the bureau service which is due end of January 2017 and will highlight additional monitoring requirements to mitigate this risk. Key will be the capture of personal data at a lower threshold.

4. Suspicious Activity Reporting (SAR) failure:

- The Promontory review at the end of 2015 and the risk assessment by Thistle Initiatives in 2016 highlighted that the current paper reporting process is cumbersome and poorly completed, with forms sent by post and at risk of loss or delay. Information is often missing from the forms and all forms have to be scanned and manually logged onto a database, prior to being manually input to the NCA portal, if disclosure is required.
- Controls currently in place include:
  - All non-disclosed SARs are reviewed monthly by the Head of Financial Crime and a sample of disclosed SARs are reviewed for completeness.
  - Additional NCA training and guidance has been provided to the Fraud Analysis Team who undertake SAR review and disclosure.
  - AML/CTF training covers SAR requirements.
- The volume of SARs received and disclosed is monitored monthly. Generally the volume of SARs received is increasing year on year (c15% 2015/16-2016/17). Quality issues mean that outbound calls are required to ensure reporting standards are met. Nevertheless, SAR capture and disclosure has improved over the period.
- Current controls are partially effective and a project has commenced to provide further enhancements due early 2017, with the replacement of paper reports with telephone reporting via Grapevine which will improve data and reporting quality at point of capture and remove operational inefficiencies.

5. AML/CTF Resourcing:

- The Promontory review at the end of 2015 and the risk assessment by Thistle Initiatives in 2016 highlighted that the resourcing within Post Office to meet its regulatory obligations was insufficient both in terms of relevant skills and experience and in terms of resource to undertake effective monitoring and management.
- The controls currently in place are :
  - Key personnel within the Financial Crime and Fraud Analysis Teams undertook formal regulatory training during 2016;
  - All regulatory activity and workloads are reviewed at the monthly Financial Crime Governance Forum;

POL00247018

- There is an HMRC Steering Group to review the current HMRC audit and also the progress of the financial crime risk assessment work being undertaken; and
- A new Fraud, Loss and Crime Forum has been established where AML/CTF operational issues are highlighted.

- An annual training and communications plan relating to AML/CTF requirements is developed each year, and the 2017/18 version is being enhanced with different training elements. Additionally, a more targeted approach is being developed to ensure that branches receive training specific to their needs – particularly where they have high volumes of regulated transactions.
- The issue of resource (in terms of headcount and systems) is being reviewed and assessed as part of the risk mitigation work.

6. Bureau de Change business relationships

- The current Bureau de Change service is for occasional personal use, although this does extend to individuals undertaking occasional business travel. Historically, offering Bureau de Change services for businesses had been allowed by the AML team and encouraged by sales teams, despite the inability to perform full due diligence, beneficial ownership and PEPs & Sanctions checks. This was restricted during 2015-16 via branch communications and the 2016 AML/CTF training, however from monitoring, it is evident that certain branches continue to offer services for business without full customer due diligence being undertaken.
- These transactions cannot be prevented via Horizon, and the actual volume can only be estimated due to data and systems limitations. Controls currently in place include:
  - The Fraud Analysis team review all SARs and any transactions over £5,000 to identify business transactions, and
  - The Financial Crime team investigate referrals from stakeholders including the Fraud Analysis team and FRES and take appropriate action to mitigate.
- Accordingly, the current controls are only considered to be partially effective. Thistle Initiatives are completing a risk assessment of the bureau service which is due end of January 2017 and will highlight additional controls and data required to mitigate this risk.

POL00247018

Appendix 2 – Preliminary Findings from the Bureau de Change product review

Subject to completion of the project early 2017

- Establishment of a strong working party from the outset with defined Terms of Reference to achieve the shared goal – this was not possible for Bureau de Change due to access to key staff
- Key accountabilities must be defined and members must have sufficient delegated authority to enable recommendations to be delivered
- Each business area must clearly document their operational policies and controls to support policies in relation to prevention of financial crime
- First, second and third line of defence controls should be clearly articulated, resourced and tested on an ongoing basis with rationale for adequacy clearly documented
- Current operations lack sufficient resource, and IT infrastructure is poor and too outdated to undertake sufficiently granular testing or analysis
- Ownership and responsibility for all aspects of control throughout the product lifecycle and the process flow of Bureau de Change should be formally documented
- Contractual obligations should be brought up to date to reflect current operations and to take into consideration legislative changes including PEPs and Sanctions;
- data capture and ID&V for Bureau de Change transactions below the current level of £5k must be enhanced
- Current control processes are predominantly manual and this restricts the level of interrogation possible compared to that which HMRC have been able to undertake; their findings will drive next steps in this regard
- The volume of €500 buy transactions within branches without dispensation is higher than acceptable but is currently dependent on manual controls. Monitoring is therefore ineffective, and more automated controls should be considered. If the intention is to continue to receive €500, then screen prompts should be introduced as an interim fix beyond more sophisticated IT improvements
- Introducing new ID&V thresholds will help control the current risk of splitting transactions but system changes would need to be introduced to ensure better quality data capture
- Whilst £10k transaction breach reporting and mitigation activity has improved, identification remains manual and system changes are necessary to further control this risk, supported by new ID&V data capture
- System enhancements to the Horizon basket settlement process should be considered, as currently multiple transactions can be performed in the same basket, culminating in breaches of the £10k limit
- A risk based approach to undertaking customer due diligence (CDD) and enhanced due diligence (EDD) including PEPs and Sanctions checks must be determined as a priority, especially in light of the new requirements for UK PEPs under the 4th MLD legislation that is due June 2017

POL00247018

- Automated solutions for CDD and EDD, including adopting the current API link to FRES used for Travel Money Card and relying on third parties to undertake the checks should be considered and costed
- A sample of PEPs and Sanctions checks on 30 high value bureau transactions has been undertaken, but is too small a sample upon which to establish a risk based opinion and HMRC findings will not be established until the end of January. Given the volume of transactions, to extend this sample to a realistic level (say 5%) would require significant resource, and therefore the approach to PEPs and Sanctions checks needs to be based on a qualitative rather than quantitative basis.
- Eddie Jarman, as product manager for Bureau de Change is raising a change request to explore the options and associated costs of the various IT enhancements that may be required
- All enhancements to data capture and associated robust controls will need appropriate resource to undertake testing and analysis, which will not be possible within current headcount
- BFPO activity is not relevant to Bureau de Change and will be reflected in the assessment, more broadly all Product Managers should have sufficient understanding of BFPO arrangements to determine any associated risks including financial crime to their product or service

POL00247018

Appendix 3 – Preliminary Findings from the ABC review

Subject to completion of the project early 2017:

- Thistle have found strong written and practiced procedures in many areas of business including network, supply chain and procurement
- Public procurement is a particularly robust process and less of a risk than private procurement for POMS
- Greatest inherent risk of bribery would appear to be at branch level owing to the use of third parties and potential financial crime risks in general
- Impact of such risks to the business would be low in the main
- Significant ABC network risk would be better controlled in terms of reducing the attractiveness of bribery or introducing stronger deterrents including consequences if caught
- Adopting stronger controls in relation to financial crime risks such as AML, would naturally have a positive impact on the likelihood of ABC risk occurring, particularly in the Network
- Initial findings have found a strong cultural integrity embedded within Post Office, with an understanding of the importance of the reputation of Post Office as a community, government funded business
- Culture is reinforced with ongoing training, high level procedures and contractual obligations
- Weaknesses have been identified with elements of the training and a lack of recorded documentation of operational procedures.

POL00247018

5.1) MLRO Assurance Report July 2015-Dec 2016

Author: James Dingwall Sponsor: Jane MacLeod Meeting date: 30th January 2017

Executive Summary

Context

The Money Laundering Regulations require the Money Laundering Reporting Officer (MLRO) to report annually on compliance with the Money Laundering Regulations 2007 (MLRs) and The Terrorism Act 2000, including significant incidents, potential gaps or weaknesses that required further investigation and further recommendations, if appropriate, on remedial actions to close such gaps in accordance with senior management risk-appetite.

Questions this paper addresses

- What is the Anti Money Laundering (AML) Governance Framework within Post Office Ltd and how is it performing?
- Are systems and controls operating correctly?
- What are the recommendations for action?

Conclusion

1. Due to limitations with current data capture processes at point of sale ('POS') and analysis capability, the current Bureau de Change transaction monitoring is considered ineffective. It is likely to be criticised in the Her Majesty's Revenue and Customs (HMRC) report due in January 2017.
2. Post Office Ltd must balance the competing requirements of Network Access against risk management and mitigation; this is a particular challenge where the vast majority of Post Office branches are independent businesses. Under current Post Office Ltd practices, the consequences of a branch failing to comply with regulations can be significantly drawn out and subject to commercial influences.
3. Managing and controlling financial crime risk within Post Office Ltd is reactive and incident-responsive in the main and there is insufficient resource internally to adopt a significant proactive approach commensurate with the assessed risk.
4. Agency office staff operate outside standard 'banking' environments, in that post masters/mistresses are usually self-employed, there is "no on the ground" one to one supervision. This isolation potentially creates an environment in which the normal peer to peer constraints and oversight are largely absent.
5. This situation creates the potential for conflict to exist in a busy branch environment between customer service and process compliance, particularly where a transaction might require capturing additional information or the branch staff may be suspicious. Proposed solutions in this regard are invariably system-

POL00247018

led, time and cost expensive and constraints exist in relation to the capabilities of the current Horizon IT system.

6. Post Office Ltd is heavily reliant on manual analysis of data via excel spreadsheets and is severely hampered by inadequate Information Technology (IT) infrastructure. Access to appropriate and timely Management Information (MI) is frequently dependent on third parties.

7. The current risk appetite for Post Office Ltd ('averse') has been set at a high level and does not take account of the level of change underway. While the number of issues to be addressed is significant, these must, and can be prioritised.

8. Considerable work has been done during 2016 to assess the AML and Counter Terrorist Financing (CTF) risks to which Post Office Ltd is exposed. An action plan has been developed in relation to product/service specific risk assessments; an increase in financial crime resources has been recommended; and there is clarity in terms of the business's commercial objectives and new leadership is driving the business forward. Following completion of the majority of Phase 2 of the Financial Crime Risk Assessment project during 2017, Post Office Ltd should consider whether the generic 'averse' risk appetite remains appropriate or whether a more granular approach should be explored.

9. Post Office Ltd should be able to demonstrate robust decision making in terms of its financial crime risk control environment. Using enhanced MI will allow Post Office Ltd to more accurately assess commercial objectives alongside its financial crime exposure. This will allow the business to decide which products should be addressed as a matter of priority and to create a specific action plan in relation to each prioritised product.

10. The results of the pilot exercise in relation to Bureau de Change are expected in January 2017, as is the audit report from HMRC (See the separate Annual Risk Review Report for January 2017).

Recommendations for Action

11. Post Office Ltd needs to decide where operational responsibility sits for completing the risk assessments on an ongoing and product/service specific basis, for new, upcoming and existing products/services.

12. 1st line policies and procedures are not sufficiently mature to meet the demands of the regulated environment. These need to be enhanced and implemented, together with robust assurance and control.

13. Post Office Ltd currently has insufficient resource to complete the risk assessment mitigation and review and assess the impact of the new Money Laundering Regulations when they come into force in 2017. Owing to these limited resources, Post Office Ltd is prevented from enhancing its level of transaction monitoring. These resourcing constraints need to be taken into consideration when prioritising actions.

Input Sought

The Committee is asked to note the content of the MLRO report set out in this paper.

POL00247018

The Report

This report addresses the following:

A. Purpose and Scope of Report
B. Background
C. Governance Framework
D. Operation and Effectiveness of the Control Framework, including documentation of policies and risk assessments
E. External threats/Landscape

A. Purpose and Scope of Report

14. HMRC is the regulator responsible for supervising compliance with MLR requirements. Their oversight relates to Post Office Ltd Money Service Business (MSB) activity, specifically, the provision of Bureau de Change and bill payments.

15. The MLRs clearly identify an expectation that MSBs should adopt a risk-based approach to the prevention of money laundering and terrorist financing. This approach is a question of senior management judgement, to be determined in the context of the particular risk facing the business.

16. The purpose of this annual report is to appraise senior management on key Anti Money Laundering and Counter Terrorist Financing (AML/CTF) activity being undertaken in the Post Office; providing an informed insight into the risks identified in the operating environment. The report will comment on the effectiveness of systems & controls; reporting on their implementation and effectiveness throughout the firm, comments on significant incidents, potential gaps and weaknesses identified, and make recommendations and suggest remedial actions to close gaps so that senior management can then consider any prioritisation of actions that may need to be taken in order to operate within Post Office Ltd's risk-appetite. An additional assessment will be undertaken concerning Post Office Ltd's principal firm Post Office Management Services; a report on which will be produced early 2017.

B. Background

17. It should be acknowledged that significant progress has been made in Post Office Ltd following the appointment of the new chairman, Tim Parker, in October 2015 and the resultant change in the direction in which he is leading the business. In terms of the financial crime risk environment, the improvements resulting from the changes introduced under the leadership of John Scott (MLRO), with the guidance and assistance of Sally Smith (Head of Financial Crime), should also be acknowledged.

18. Nevertheless there are recognised constraints, not least of which is the continuing network and business transformation. However, within the wider Financial Crime team, including the Fraud Analysis team in Chesterfield, there is a general culture to achieve the best possible outcomes with the tools available.

19. Following identification of significant breaches in July 2015, the General Counsel commissioned a review by Promontory of the Post Office AML/CTF Framework. In

POL00247018

February 2016, HMRC advised that they would be conducting an audit of the Money Service Business in respect of which Post Office is directly regulated for (subsequently determined to be Bureau de Change and Bill Payments – Supply Chain MSB cash collection clients were removed once the decision was made to exit the external cash market). Their audit has been delayed (due to resource issues within HMRC) and the report is now due in January 2017, however, this is expected to find a number of deficiencies relating to Bureau de Change activity. Thistle Initiatives Limited were contracted in July 2016 to assist with risk assessment work across the products and services from a financial crime perspective.

20. Post Office's business model means that a majority of its products offered are through third party white label solutions and joint venture arrangements. As such, direct regulatory risks are focused predominantly upon Bureau de Change, Bill Payments and Drop & Go. Notwithstanding these arrangements, the most significant impact of financial crime on Post Office is reputational damage. Negative media attention following an incident of financial crime has potential for consequential devaluation of brand values and the possible impact on Government commitment which is vital to support Post Office culture and the business.

21. At the end of 2015, it was identified that there were issues with the registration of Post Office branch premises with HMRC, particularly in relation to mobile outreach services that had never been registered. These registration anomalies were raised with HMRC at a meeting in February 2016 when clear guidance on which premises were registrable was sought. Subsequently clear business rules were defined and agreed with HMRC, and at annual renewal in June 2016, a complete refresh of premises registration against the new business rules was undertaken, as below:
    - 10,236 branch registrations required amendment due to the addition of "Bill Payment" as one of POL's regulated activities
    - 951 premises that were in long-term temporary closure status needed to be de-registered
    - 576 premises were registered for the first time, including:
        - 41 mobile van outreach services (MOB), for which back fees were due, and
        - 417 mobile kit outreach services (HOST, STORE and PART), category registered for the first time 1st June 2016.
    - Of the remaining 118 premises, the reasons why these branch premises were previously excluded from registration with HMRC are set out below:
        - 5 of these branch premises have no public access and were therefore excluded from branch premises registration
        - 57 of these branches are greenfield premises (Crown, Local and Main) that were historically omitted in error
    - The remainder of these branch premises were previously deemed to be out of scope by Post Office, majority being the branch type – Scale Payment Sub Office Branch (SPSO) - 56 branches

22. Post Office Ltd is now awaiting a pre-penalty notice from HMRC in relation to these historical premises registration errors, although we have been advised that the de-registrations will be excluded, therefore the likely penalty should be no more than £500k.

POL00247018

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

23. The previous Money Laundering Reporting Officer (MLRO), John Scott, left Post Office Ltd on 30th September 2016. James Dingwall was appointed as Post Office Ltd's interim Money Laundering Reporting Officer with effect from 30th October 2016, with a permanent MLRO expected to be appointed in early 2017. James Dingwall has delegated day to day MLRO oversight to the Head of Financial Crime, Sally Smith. Both are located in Finsbury Dials, Moorgate, London where Post Office Group head office is situated.

24. The MLRO is the focal point of all AML/CTF activities within Post Office Ltd and with the assistance of the Financial Crime team is responsible for assessing Post Office Ltd's exposure to financial crime. This responsibility includes making decisions regarding the submission of suspicious activity reports to the National Crime Agency (NCA) or law enforcement; whether to proceed with the reported transaction, and what information may be disclosed to clients or third parties. Due to the fact that the MLRO is at present an interim appointment, procedural arrangements are in place to ensure that Head of Financial Crime is able to act on behalf of the MLRO where required.

25. With the assistance of the Financial Crime team, the MLRO takes ultimate responsibility for the provision of training within Post Office; advising on how to proceed once an internal report and/or SAR has been made and the design and implementation of internal anti-money laundering systems and procedures.

26. The MLRO is restricted in carrying out his function as this is an interim position and as such he lacks permanence to be able to enforce long-term goals. Cost reduction measures since 2014 have created risks due to the loss of skilled staff members and the resulting loss of product and business knowledge; as a result, Post Office often relies upon contractors to fulfil core roles.

27. Legacy IT systems such as Horizon constrain the ability of staff to gather accurate Management Information to ensure that the business correctly identifies and complies with its regulatory obligations.

28. Following the transfer of the AML function in 2015, a monthly operational governance meeting was established at the end of 2015 to ensure adequate MLRO oversight of AML/CTF investigations, non-conformance by branches or individuals, training & communications and any other regulatory issues at a granular level. The forum also ensures that issues are escalated to senior management within the business, as appropriate. During 2016 regular reports have been provided to the Risk & Compliance Committee and the ARC relating to AML/CTF controls, the outcomes and recommendations of the Promontory Review reported in January 2016, the Thistle initial Risk Assessment in October 2016, and the current HMRC audit.

29. Currently, outside the Financial Crime team, financial crime MI reporting is not at a sufficiently granular product level to aid transparency and decision making at an operational level. Thistle Initiatives Limited's Financial Crime Risk Assessment was not able to evidence that the MI that is gathered sufficiently supports a consideration of trends and benchmarking at a product/service level. As a result, there is a risk that decision making within the business does not have sufficient information and analysis to appropriately balance commercial considerations against regulatory risks.

POL00247018

30. The results of HMRC's 2016 audit of Post Office are expected in January 2017, however from discussions with the auditor it is expected that a number of comments will be made by HMRC in relation to our MI and our analysis of any data.

31. Irrespective of whether the Financial Crime Team owns the management and maintenance of financial crime risk controls or whether these are delegated to a product or service operational level, Post Office management should understand the extent of the financial crime risks posed across the business and the effectiveness and/or deficiencies of the mitigating controls. Both management and second line should ensure that the controls in place work as intended.

32. In managing its financial crime control risks Post Office Ltd faces a number of business-wide constraints which do not relate specifically to individual products and services but which nevertheless impact on the business's overall ability to manage the financial crime risks to which it is exposed. Some are already well documented (see the MLRO's AML/CTF report 2014/15)

33. Additionally, the 2013 Detica Report (BAE Systems Detica undertook an assessment of Post Office Ltd's systems and controls in place to address fraud and proof of concept in 2013) highlighted significant weaknesses in the IT capability and made recommendations for improvement. In particular, they identified that the technology available to central operational teams was not fit for purpose; and analysis of large data sets continued to be performed on an ad-hoc basis of data subsets copied into Excel. These concerns were addressed in the specifications for the IBM Front Office replacement system, however with the termination of the contract, these issues remain unresolved.

34. A new operational Fraud, Loss and Crime forum was established in November 2016 by the Chief Finance Officer (Al Cameron) to understand the impact of financial crime loss and to ensure that remediation activity is managed effectively and proportionately across the business.

D. Operation and Effectiveness of Control Framework

35. At the core of the MLRs is a requirement for Post Office to maintain appropriate and risk-sensitive policies and procedures relating to:
    - Customer due diligence (CDD)
    - Reporting of suspicious arrangements/transactions
    - Record keeping
    - Internal control
    - Risk assessment and management
    - Monitoring and management of compliance
    - Internal communication of policies and procedures
    - Processes and on-going monitoring

Customer Due Diligence

36. There is an overriding responsibility for Post Office Ltd not to fall foul of relevant legislation in relation to Sanctions and Politically Exposed Persons (PEPs). Post Offices' AML/CTF policy states that it will take a risk-based approach to sanctions and PEPs checking. While this is a reasonable and justifiable approach, Post Office

POL00247018

should formally record where risk assessments have been made and any specific decisions based on such assessments.

37. With the exception of travel insurance and supply chain MSB clients, Post Office itself does not currently conduct either Sanctions or PEPs checks; instead it relies on the third party provider of those products to conduct such checks – for example, Bank of Ireland for financial services products, First Rate Exchange Services (FRES) in relation to online bureau services, Moneygram and third party banks. In light of the changes proposed in the 4th Money Laundering Directive, Post Office is currently considering if it is able to utilise an existing Application Programming Interface (API) link to a third party created for the new Travel Money Card to undertake automatic PEPs and Sanctions checks for Bureau de Change customers. Next steps include appropriate due diligence and determining the resource and costs involved.

38. Acceptable identification and address verification documents are detailed on Horizon and within the AML/CTF training workbook supplied to all branches. There are no exceptions to these documents. The ongoing HMRC project has highlighted Post Office may need to reconsider the current protocols for collecting customer data. Specifically in relation to Bureau de Change transactional data capture, and then Identification and Verification (ID&V) processes.

39. Outsourcing our Sanctions and PEPs screening will not however, reduce or remove our regulatory obligations. Post Office still has a responsibility for ensuring that the checks completed are correct, timely and any failings of the third party checks would rest with Post Office. A more detailed review should be undertaken to consider full business impact in introducing changes including:

- Data capture for all transactions
- Reducing the current levels of ID&V checks
- Introducing limitations to cash On Demand transactions

40. Currently Post Office is only able to proactively monitor Bureau de Change transactions over £5k, or where the clerk has pressed the 'suspicious activity' button and input the customer and ID details. A daily file of this information is provided to the Fraud Analysis Team in Chesterfield who undertake manual monitoring via Excel spreadsheet to identify linked transactions or suspicious activity which is then raised to the Financial Crime team and MLRO as required who make the final decision as to which incidents are disclosed to the NCA [See *Annex; Report on duties of nominated officer* for additional information]

41. Tattersalls at Newmarket [1] is currently the only commercial relationship in operation for Bureau de Change activity and in view of HMRC focus, a review of the due diligence process for this customer was undertaken by Thistle Initiatives Limited. As bloodstock auctioneers, Tattersalls is itself regulated for Money Laundering purposes in the UK and as such it could be argued that Simplified Due Diligence ('SDD') is appropriate. However as this business relationship is predominately in relation to 'buy back' €500 notes (currently controlled through a single Branch relationship) which are seen as high risk notes, Thistle Initiatives Limited considers that additional due diligence should be considered as prudent risk based control, including:

[1] *A historic relationship for which due diligence has been performed as a one-off*

POL00247018

- commercial bureau de change is a high risk product and Post Office cannot currently evidence that it has considered the requirement to undertake more enhanced due diligence;
- Post Office should formulate an approach to and the application of ongoing due diligence for business relationships;
- there is insufficient information to confirm that Post Office has identified the ultimate beneficial owners of this firm;
- there are insufficient records to support why Post Office decided that identity documents for only two of the seven Directors would be sufficient for the purposes of CDD; and
- If finalised as expected then one of the Directors would be captured by the new PEP requirements in Fourth Money Laundering Directive (4MLD); requiring Post Office to document that this has been identified and their rationale for deciding to accept the risk of conducting business with a PEP should Post Office continue to do so.
- Formal recording of the basis on which the decision was taken to accept €500 notes and the controls developed to monitor this relationship and mitigate identified risks. Separately, Post Office should ensure that sufficient controls exist in relation to Tattersalls or other future relationships to understand the parameters of their own activity and are aware of the risks of straying into other regulated activity (e.g. acting as an MSB).

Reporting of suspicious arrangements/transactions

42. All suspicious activity reports are reviewed and, where appropriate disclosed. This activity together with monitoring of Bureau De Change transactions over £5k is undertaken by the Fraud Analysis Team in Chesterfield under oversight by the Head of Financial Crime. The Financial Crime Team support more detailed investigations via liaison with relevant stakeholders. *(See Annex: Report on duties of nominated officer for additional information)*

Record keeping

43. All record keeping relating to AML/CTF is electronic (all Suspicious Activity Reports (SARs) and paperwork are scanned and saved electronically) and filed within a restricted access AML drive under the control of the Head of Financial Crime.
44. In undertaking the Financial Crime risk assessment, significant weaknesses in record keeping were highlighted, some of which were already being addressed. An exercise had previously started in 2015 to establish a centralised document repository however an appropriate infrastructure was not completed due to resource constraints. Accordingly, responsibility for underlying policies and procedures continues to rest with each business area, and there are known inconsistencies in the length for which records are retained (the regulatory requirement is to retain records for a period of five years). Significant changes in structure, transformation and resources in terms of technical capability and personnel have continued to weaken the record keeping infrastructure. Information Security and Assurance Group (ISAG) have been notified of the regulatory requirements for data retention and this is to be tackled as part of the ongoing product and service assessments in relation to financial crime.
45. The challenge of locating key records has undermined a significant number of controls because it is not possible to fully evidence procedures and compliance with them - for example, which party is responsible for ensuring, where applicable,

POL00247018

that the business does not deal with Politically Exposed Persons, who is checking against the sanctions list, what MI either party is required to produce, how often and why, what record keeping applies.

46. A project is underway to centralise the retention of all signed current and dated contracts/agreements, and contractual arrangements with third parties must clearly set out the responsibilities of both Post Office and the relevant business partner where a third party is involved in product/service delivery. As part of the continuing commitment to undertake a risk based approach to product risk assessment, it is expected that record keeping requirements will fall within the remit of the Product manager.

47. An exercise to retain records in relation to transactional MI which would have facilitated trending and analysis in relation to financial crime controls did not proceed due to constraints in relation to data retention capability and resource.

48. The processes and controls relating to branch premises registration have been reviewed and enhanced to ensure that there are no future regulatory failures with this process.

49. Court Orders - Post office has received 36 Data Protection Act [DPA] requests for information from Law Enforcement and regulatory bodies from June 2015 to December 2016. 29 of these related to high risk MSB clients within the Supply Chain external cash market. Of the remaining 7, these were split across MoneyGram, fraudulent card transactions and Postal Orders.

Internal Control

50. Post Office relies on a variety of internal controls as follows:

Appropriate Employee Training
All customer facing staff are required to complete mandatory annual AML/CTF training. In 2016, for the first time, this annual training was extended to all employees, and a back office module was launched in March 2016. In February 2015 Post Office Security assumed responsibility for the AML and CTF function within Post Office Ltd. A Communication Plan was developed with a view to rolling out:

- annual mandatory baseline AML training to branches, cash centre staff and customer support centre staff
- bespoke mandatory AML training to high risk audience groups including relevant product managers, Finance, Crown and network area sales managers, FSC, Cash Management, NBSC, Supply Chain Sales Managers and Security
- bespoke mandatory training to those branches that are permitted to accept EURO 500 notes (circa 46 branches)
- an awareness and communications calendar that raises awareness across target audience groups of AML and CTF, along with the key behaviours that should be demonstrated to maintain compliance
- The development of metrics to evaluate AML awareness and communications success and provide a process for identifying and building improvements.

51. Current monitoring of training completion levels is manual and labour intensive, although this is expected to be resolved with the Success Factors platform.

POL00247018

Completion levels of AML/CTF compliance training delivered during 2016/17 are as follows:

- Back/Head Office Training – the current system is showing that a small percentage of employees have failed to complete the annual training. However, the annual training is due in March 2017, and the new learning platform has improved completion reminder tracking.
- Directly Managed and Agency Branch Training – Directly Managed completion is 100%. The Network Branch Standards team are arranging calls to branches to chase any outstanding training completion.
- Supply Chain – annual training being rolled out January-March 2017, and completion will be reported to Risk and Compliance Committee (R&CC).

52. Aspects of the current training material including key aspects of customer journey and financial crime training are not flagged as due for review; however they do contain out of date material such as the New Entrants Training Workbook which makes reference to products that Post Office Ltd no longer provides; including Motor Vehicle Licences.

53. Whilst the roll out of Success Factors will provide a training platform for back office staff and associated contractors. The programme has not yet been rolled out across the agency network, and timescales to achieve this are not yet known. The Network will instead continue to rely upon Horizon based online training modules, and Supply Chain staff will continue to utilise Work Time Learning Sessions. The disparity between the use of Success Factors for back office functions and the use of alternate training portals for the remaining areas of the business will pose issues regarding identifying which individuals have completed the required training.

54. It was agreed at the November R&CC that completion of mandatory compliance training will be a gateway requirement for bonus payments. It is proposed that a communication to this effect will be issued by General Executive (GE) in January 2017.

55. New Training, Awareness and Communication Plans are scheduled to be rolled out during Q4; this will include annual mandatory training, refresher training for branches or individuals where compliance breaches or issues are identified and on-going awareness via Branch Focus, One and the Grapevine website.

56. During 2016, the following formal training was completed by the Financial Crime team:

- John Scott (MLRO till 30th September 2016) completed the AML Advanced Diploma
- All the Financial Crime Team and most of the Fraud Analysis Team completed the International Compliance Association (ICA) AML Certificate
- The Financial Crime Team and the Fraud Analysis Team attended an in-house workshop led by the NCA. Additionally, the NCA visited Chesterfield twice to provide support and guidance relating to SAR disclosure

57. Fit and Proper tests have been performed on all external Board Directors, GE and the MLRO as required.

Risk Assessment

58. Policies relating to Financial Crime overall and AML/CTF specifically were approved during 2016, and are the subject of a separate Annual Review

POL00247018

59. Processes within the Financial Crime and Fraud Analysis Teams are robust and up to date, however processes and policies across the business to support these are less mature and require improvement

60. Following identification of a number of issues and breaches in 2015, Post Office requested that Promontory Financial Group (UK) Limited review its AML and CTF framework at the end of 2015. A key finding from the report was the need to undertake a business wide formal risk assessment. Thistle Initiatives Limited were appointed to undertake a product specific Financial Crime Risk Assessment across 63 products in July 2016, the findings from which were reported in October 2016. The aim of the review was to leave Post Office with a legacy which allows the business to manage its financial crime risk environment going forward.

61. Based on the findings from the report, next steps for Post Office were based on a risk based approach, selecting Bureau de Change as the highest risk, upon which to conduct a deeper dive review. These next steps were aligned with the business's product/service objectives – i.e. expansion, consolidation, etc. In addition, factors such as contribution to income, volume of sales, level of financial crime activity, community considerations, Post Office Ltd funding, should all form part of the Post Office decision making process.

62. The final report from Thistle Initiatives Limited is due shortly. After the completion of the Bureau de Change pilot exercise Post Office will need to determine whether, how and to what extent it is prepared, and able, to address the risks identified in the assessment in terms of control mechanisms and allocation of resources, including information technology systems.

63. Post Office is heavily reliant on manual analysis of data via excel spreadsheets with little supporting MI infrastructure. Access to appropriate and timely MI is also frequently dependent on third parties.

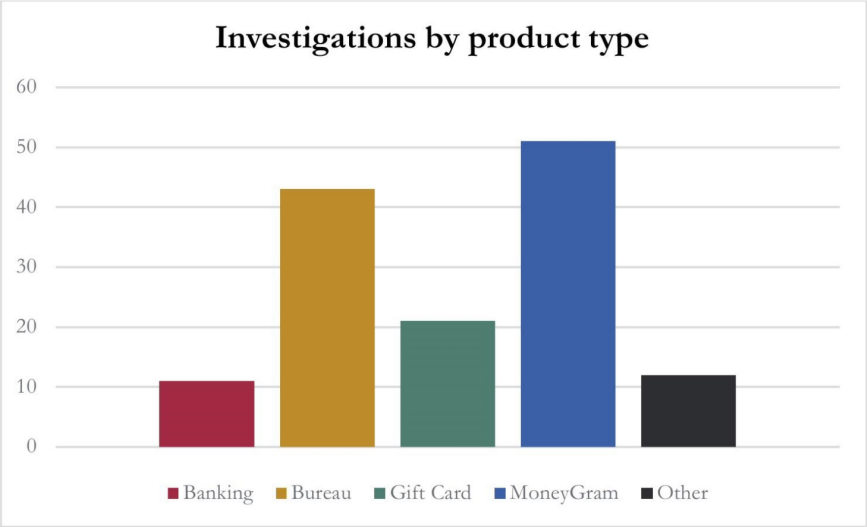
64. In addition it appears that a Data Dictionary for Horizon and Credence that fully documents field content and uses cannot be located by IT. This is a concern as it means that Post Office is reliant on Fujitsu controls in relation to data understanding and availability. Post Office is currently unable to provide an overview of where data is stored within the systems albeit there is an awareness of which data must be stored however the fields cannot be located for reporting purposes. Requests to Fujitsu in terms of data location will invariably be subject to a cost benefit analysis prior to submitting a request.

High Risk Products and Services

65. Bureau On Demand is the highest risk directly regulated product for Post Office:
    - Transactions over £10k within 90 days for the same customer
    - Transactions being structured through splitting the transaction up in order to be processed below ID&V requirements
    - €500 Notes being accepted outside of the permitted branches (circa 46 branches)

66. Between June 2015 and December 2016 the Financial Crime team completed 138 investigations, the graph below provides a breakdown by product.

POL00247018



Bureau de Change [2]

67. During 2016/17 year-to-date (20/12/2016) there have been 43 investigations relating to branch non-conformance and confirmed card fraud. As of December 2016, there are 14 branches on manual reduced thresholds as a result of serious non-conformance. The majority of these relate to transaction splitting (in order to avoid the ID threshold) and branches not conforming to the regulatory limit of £10k per customer, cumulative over a 90 day period.

68. In May 2016, a significant spike in card fraud was identified around the London area (5 branches, c£360k). The majority of cards were issued by NatWest bank and obtained by criminals using different courier fraud scams (fraudsters call and trick (normally vulnerable) individuals into handing over their cards and PIN numbers to a courier). Each branch was visited and education and training was provided with the Postmasters/Managers, they were also advised to complete a 'Walk Away' test and 'Code 10' on all bureau transactions over £1,500. Information was shared with NatWest bank and London Metropolitan Police which resulted in a suspect being detained. In response to this sudden spike, a network wide communication was sent out to reinforce awareness of card fraud and best practices. Numerous Area Sales and Field Teams conference calls were also attended to raise awareness and to share best practices.

MoneyGram [3]

69. There has been an increase in the level of card fraud since Post Office started to accept card as a payment method in October 2015. As you can see from the

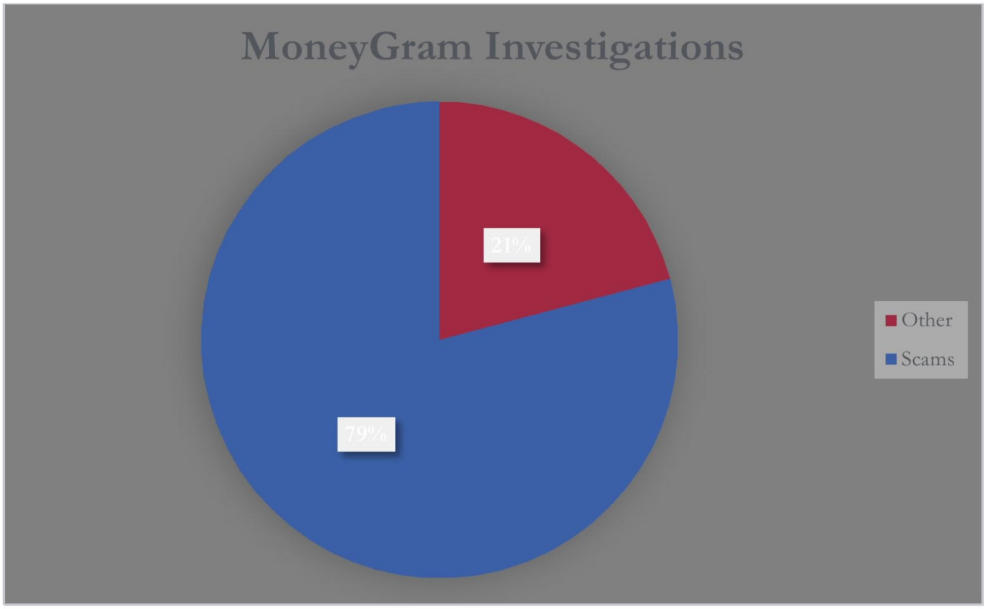
[2] *volume and value of branch transactions 2015/2016 7.5m & £1.9bn, and to P6 2016/17 4.3m & £1.1bn.*

[3] *volume and value 15/16: send transactions 3.1m & £769m, receive transactions 342k & £100m. Volume and value to P6 16/17: send transactions 2.2m & £586m, receive transactions 236k & £80m.*

POL00247018

graphs above the majority of investigations and SARs raised have been associated with the MoneyGram product.

70. There has been an increasing trend of vulnerable customers falling victim to 'Talk Talk' or 'Microsoft' scams. This has been reported via branch SARs, calls to Grapevine and from notification received directly from the card issuers. As you can see from the chart below, 79% of investigations relate to customers being victim of a scam.



71. During 2016, there was a spike in SARs from the network, reporting that vulnerable customers were sending money to Georgia. This was escalated to MoneyGram who blocked these fraudulent receivers. MoneyGram have since also placed a limit on the amount that can be sent to Georgia.

One4All Gift Cards (GVS) –

72. In 2015/16, a group of individuals purchased multiple One4All gift cards by cash and card. These gift cards were being used to purchase baby milk from Boots (Online) and subsequently being sold and shipped to China for a much higher price. Due to this suspicious activity an internal risk assessment was completed and it was agreed by the MLRO to refuse any future sales. This information was shared with HMRC who are investigating further.

73. There has also been an increase in customers purchasing high volume of low value gift cards (i.e. 30x £24 gift cards). The gift cards were being purchased with either cash or card and then converted online into Amazon gift codes and MasterCard virtual money. This suspicious activity was quickly escalated to GVS to review. In cases where the money had not yet been spent, GVS blocked the funds - none of these customers have called to enquire about the block. GVS will complete due diligence checks if these individuals make contact.

POL00247018

Banking (Deposits)

74. This year there have been multiple incidents of individuals depositing large volumes of cash over Post Office counters. SARs have been raised by branches due to their suspicions, with volumes deposited and from the conversations they had with customers about the nature of their business.

75. In particular, one customer had been depositing large amounts throughout the year but increased their frequency in August 2016. This was escalated to Santander, who confirmed they were reviewing the accounts. The amounts varied in value and in one instance they deposited c.£250k in one day. Between August and September the customer deposited c.£4million. It was agreed by the MLRO that whilst Santander reviewed the accounts the Post Office should decline any deposits over £100,000 per week as agreed as part of the Location Exercise. All SARs have been shared with Santander and disclosed to the NCA.

MSB Clients

76. During the summer of 2015, following Law Enforcement requests for information relating to several of the 15 Supply Chain external cash clients involved in MSB operations, a review of the portfolio was undertaken at the instigation of the MLRO, John Scott. This review identified gaps in the due diligence and monitoring controls in place, including the fact that PEPs and Sanctions check requirements had not been considered. A licence for Thomson Reuters Worldcheck system was procured and all relevant directors and beneficial owners within the portfolio were retrospectively checked. Remediation of due diligence and monitoring was halted in the spring of 2016, when it was announced that Supply Chain were pulling out of all external cash collection services during Q3.

77. 29 DPA requests relating to MSB clients were received between June 2015 and December 2016, across 5 of the 15 clients.

78. In June 2016, following an investigation by the Metropolitan Police which Post Office supported for over a year, Post Office suspended and terminated one of the external MSB Supply Chain cash clients. The investigations by the Metropolitan Police culminated in the c.£4m seizure of the external MSB's assets from Post Office cash centres and 19 arrests at premises from which the MSB traded. Whilst the investigation is at present on-going under the Proceeds of Crime Act confiscation orders have been presented against the MSB, so far for £0.5m.

Product Profile

79. Post Office Limited is directly regulated by HMRC as a Money Service Business for Bureau de Change and Bill Payments. It also acts as an agent for MoneyGram (who are directly regulated by HMRC).

80. There are a number of other products and services that are sold or serviced through branches, the Internet and call centres which are provided on behalf of clients, or white labelled as Post Office. Whilst these products are regulated by the Financial Conduct Authority (FCA), the client or supplier is responsible for the regulatory activity. Post Office Ltd is required to meet its contractual obligations to them, but also to report any suspicious activity direct to the NCA, as required.

81. Additionally there are two products which Post Office provides directly; Postal Orders and Drop & Go. The latter of these products requires further review and assessment to understand whether it is captured under the MLRs.

POL00247018

Development of new products

82. All new products and services have to go through the Business Readiness Assurance approval process. Business Readiness Assurance involves multiple approval points that evaluate the confidence that the business has in accepting the change into their operational environment and ensures relevant AML/CTF risk assessment.

83. There have been no significant products or services launched, however, during 2016, Post Office made the decision to exit the external customer Supply Chain business from November 2016. This included 13 customers who were engaged in MSB activity, which were the subject of an internal review and risk assessment following a number of requests from Law Enforcement and HMRC to support their investigations into potential money laundering in that sector.

Internal communication of policies and procedures

84. The AML/CTF policy is maintained on the Post Office Ltd Intranet and relevant communications are provided to all employees. Annual training, together with regular awareness communications ensures that staff have regular reminders of relevant policies and procedures.

Arrangements for monitoring effectiveness of processes, systems and controls

85. Oversight and monitoring of the effectiveness of policies, process, systems and controls through robust lines of defence is unclear. Currently audit functions through first, second and third lines of defence is not clearly articulated, allocated or resourced.

86. The Data Dictionary referenced in the Detica Report is not available for Horizon and Credence. This is a concern as it means that Post Office Ltd is reliant on Fujitsu to say what data is available. This means that Post Office Ltd is unable to show where data is stored etc. The Financial Crime team are aware that ID data is gathered for card transactions in Horizon and that this information must be stored somewhere, however the fields cannot be located. The only way to locate these fields is to request that Fujitsu locate this data, however this can only be achieved through a formal and costly Change Request (CR) process.

E. External Threats/Landscape

Business areas

87. As stated previously, the only significant change to the Post Office landscape has been the withdrawal from the external cash Supply Chain market, and the MSB clients serviced within that sector.

Fourth Anti Money Laundering Directive

88. At present the directive is due to be implemented in the UK by 26 June 2017. When it is implemented it is expected that it will replace the existing Money Laundering Regulations – Money Laundering Regulations 2007 – and a new set of regulations will be enacted. The 4MLD will also update the Proceeds of Crime Act 2002, however the proposed changes to both the MLR2007 and the Proceeds of Crime Act (POCA) are yet to be finalised..

POL00247018

89. Post Office Ltd responded to HM Treasury Consultation Paper on the 4tMLD as follows:

- Requested confirmation from HMT that the limit reduction to €10,000 applying to goods will not apply to bureau de change services (i.e. that provision of currency is not interpreted as goods in this context)
- Requested further advice relating to UK PEPs – paper stated that they are seen as 'low risk' and their families and close associates should be treated to lowest level of enhanced due diligence (section 9.12 of the consultation paper) – given the presence within the Houses of Parliament of Post Office branches and the likely customer base being directly impacted, the guidance as to how this risk is viewed is not sufficiently clear
- Post Office Ltd do not foresee any particular issues with retaining documents electronically for 10 years instead of 5 years, but this needs to be taken in context as Post Office documentary evidence is limited due to the fact that a majority of Post Office Ltd's products and services are provided on behalf of clients and third parties. It is these clients and third parties who are primarily responsible for CDD and transaction monitoring and as such they maintain the bulk of documentary evidence. Therefore clarification has been requested to confirm if we rely on these third parties to maintain relevant documentation for 10 years to comply with our regulatory requirements
- Clarification was requested regarding the intent of the extension of the Fit & Proper test – i.e. would the test be applied retrospectively for all existing incumbents or only applied to new agents from the date of the new legislation?
- Extension of Fit & Proper tests to agents of MSBs seems appropriate for high risk money service transmission businesses where the agents do not undertake any other financial or regulated activity. In the case of Post Office Ltd however, postmasters are directly contracted agents of Post Office and are vetted as part of the on-boarding process (which includes right to work, proof of ID and address, Disclosure Scotland and other checks). Postmasters also have to undertake various mandatory training and can only perform regulated transactions through Post Office systems, which manage and define what the agent can do. It is not clear therefore what additional benefit performing an HMRC Fit & Proper test would bring.

90. Main issues for Post Office consideration include:

- Due Diligence
  - SDD will no longer be applicable in most circumstances, all transactions/clients require a degree of risk assessment to demonstrate that it presents a lower degree of risk and ongoing monitoring
  - Post Office has business relationships with local and national government, listed firms (Bill Pay Service), Credit and Financial Institutions. Whereby previously it was able to complete SDD upon these relationships, a full risk assessment will now need to be completed to satisfy the 4MLD requirements and to ensure that SDD is only completed where the risk profile confirms that this is appropriate.
  - It is most likely that Post Office will have to complete more CDD and potentially Enhanced Due Diligence (EDD) checks than it has done previously

POL00247018

- CDD requirements applicable to POMs in relation to life and related investment insurance business will need to be considered
- Post Office Ltd will need to re-consider the management of its cash-intensive clients and consider how the higher risk controls set out might affect this business.
- Post Office Ltd should consider re-examining its existing client acceptance processes and where necessary request additional documents on income or earnings, as well as setting additional documentary requirements to be met during the relationship
- Increased regulatory obligations will also led to increased costs to Post Office Ltd in terms of resource to monitor and effectively assess the due diligence information gathered. This will most likely require the recruitment of additional resources in order to complete this.
- Amendments to the Horizon system may also need to be implemented to assist with these updated requirements. The board should consider what budget can be made available to allow these changes to be made.

- Extending Fit & Proper in the MSB sector
  - It is not yet clarified if this would encompass all existing agents and branch managers, or if it would only apply to new appointments going forward and not retrospectively
  - If captured there will be significant cost to Post Office Ltd in terms of resource to manage and mitigate and the cost of undertaking the physical checks
- Electronic Money
  - Plans for Digital wallet and enhancements to Drop & Go will need to be considered
- Central Register for Beneficial Owners
  - Particularly relevant to Post Office Ltd activities such as Drop & Go
  - Post Office Ltd will be required to obtain and hold adequate, accurate and current information on their beneficial ownership, including the details of the beneficial interests held
  - Such information will need to held on a central register accessible to competent authorities
- PEPs
  - The 4MLD widens the existing definition of PEPs, in short there will no longer be a difference between domestic and foreign PEPs and EDD will always apply
  - This expanded definition will include UK MPs and Branch activity such as that within the Houses of Parliament
  - Post Office Ltd needs to ensure that it has the capability and systems in place to ensure that it can complete EDD checks and where required record PEPs accurately
  - FCA guidance in relation to PEPs will also need to considered in relation to POMs activity
- Tax crimes
  - It includes tax crimes as a predicate offence for money laundering, risk incidents include gift vouchers, Bureau de Change, drinks distributors
  - Responsibility sits with our Banking partners however Post Office Ltd should ensure any SAR related risks (e.g. drinks distributors) are being appropriately addressed to mitigate any brand association damage

POL00247018

- Also affected by Criminal Finances Bill (see below for more information)

- One off transactions
  - The one off transactional limit was set at €15k and Post Office introduced a sterling equivalent threshold of £10k; however a new limit of €10k is proposed and beyond this limit Post Office will be required to complete Due Diligence
  - Post Offices biggest risk here will be Bureau de Change business where clients require occasional services which may amount to the new threshold c£8k
  - Post Office's MI and auto reporting systems will all need to be updated to take the change into account
  - Issues in relation to non-approved Branches exceeding £10k are currently being worked through but reducing the limits further will have significant impact
  - Where outsourced to a third party, Post Office must ensure that it receives sufficient MI to confirm that checks are completed accurately and that any issues are being reported correctly

- National risk assessments
  - Post Office Ltd will need to remain aware of the National Risk Assessments and take into account any risks or issues that are identified owing to Post Office's national and regional exposure.

91. Post Office Ltd will need to complete risk assessments on all products to assess their exposure to 4MLD changes but this can only be completed once the new regulations have been finalised. There will then be an ongoing requirement to ensure that risks and any controls remain sufficient. The process of implementing an action plan to be ready for these new requirements from June next year has been initiated, beginning with seeking to identifying key individuals within Financial Services (FS), Network, POMS, Commercial (in respect of Drop & Go) who will be responsible for incorporating any new requirements into BAU processes.

Joint Money Laundering Intelligence Taskforce (JMLIT)

92. Post Office continues to participate in an information sharing agreement with the National Crime Agency. Sally Smith (Head of Financial Crime) regularly attends JMLIT meetings as a means of ensuring market intelligence and horizon scanning of issues relevant to Post Office activity can be considered on a pro-active basis.

93. In addition, all members of JMLIT are expected to analyse their internal information against the search criteria set out in requests sent by the NCA to identify, and at Post Office's discretion, disclose, relevant information to the NCA. The NCA will then analyse, and if appropriate, disseminate to relevant parties via information requests or NCA alerts.

94. Participation in the initiative was discussed during the November AML/CTF Governance Forum as invariably a considerable amount of work is required to be conducted by the Chesterfield team, the output from which very rarely affects Post Office activity; however it was determined that this is an essential relationship to maintain but the extent to which Post Office Ltd is able to contribute and the resource required to do so should be an item for consideration once the new MLRO is in situ. In preparation a review of cost

POL00247018

benefit of participation will be undertaken based on the activity undertaken during the previous 12 months.

Criminal Finances Bill

95. The Criminal Finances Bill was introduced to the House of Commons on 13 October 2016. It will significantly improve the government's ability to:
    - tackle money laundering and corruption
    - recover the proceeds of crime
    - counter terrorist financing
96. This bill is still in the first stage of being reviewed by Parliament and is at present awaiting its third reading in the House of Commons. It still needs to go through the House of Lords and receive Royal Assent. Unfortunately at this stage there is not a concrete date for when it or if it will go live. However a number of industry experts are projecting that it will potentially go live in 2017.
97. Proceeds of Crime Act 2002 (POCA) made provision for a disclosure order to assist in the confiscation, civil recovery and exploitation proceeds investigations, but as this did not include money laundering investigations this new legislation will provide a vehicle for such disclosure. Post Office Ltd should consider having an appointed person or team in place to receive these orders and action them within the required timelines.
98. The Bill will also provides two enhancements to the existing SARs regime:
    - The power to extend the moratorium period to enable law enforcement agencies to gather the evidence necessary to secure a restraint order or other intervention; and
    - The power for the UK Financial Intelligence Unit (at present the NCA) to obtain further information from SARs reporters.
99. Post Office Ltd will need to take into account the potential to extend the moratorium period as this may delay transactions or transfers where Post Office has applied for consent.
100. The Bill aims to reinforce the integrity of the UK's economy and will make sure that banks and other financial institutions are held to account for the actions of their employees. This measure introduces two new criminal offences to tackle corporate facilitation of tax evasion:
    - The domestic fraud offence – which criminalises corporations, based anywhere is the world, who fail to put in place reasonable procedures to prevent their representatives from criminally facilitating tax evasion.
    - The overseas fraud offence – which criminalises corporations carrying out a business in the UK, who fail to put in place reasonable procedures to prevent their representatives facilitating tax evasion in another jurisdiction.
101. Post Office Ltd will need to ensure that with its corporate businesses clients such as drop and go and Bureau de Change it has sufficient information to ensure that Post Office Ltd is not complicit in facilitating tax evasion.
102. Post Office has written out to approximately 400 agents where it is believed they are not downloading their VAT invoices. The reason for this is believed to be that they are not registered on the OTM online payslip/invoice service. This action was taken in response to a concern as to how agents can be conducting accurate quarterly VAT return payments to HMRC without their invoice. The

POL00247018

implications of Post Office Ltd introducing a more robust information loop linking agents remuneration to VAT receipts in HMRC is a significant challenge and will be given further consideration.

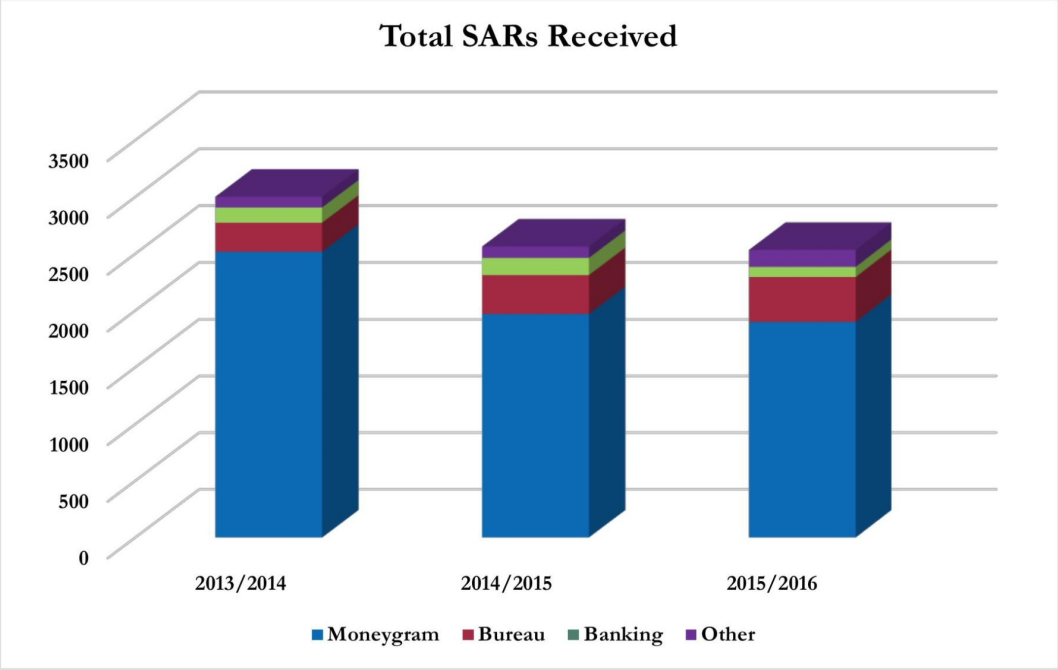
POL00247018

Annex: Report on duties of Nominated Officer

Suspicious Activity Reports (SARs) summary

A total of 2,533 SARs were received from the Network in 2015/16, compared to 2,563 the year before. At the end of 2015, a trial was commenced whereby selected branches could call Grapevine with SARs rather than complete a paper form. This was to reduce the number of completion errors, reduce the number of outbound calls to branches to collect full information/clarify report and to reduce time spent scanning and logging SARs. This trail has been successful and the process will be rolled out to the whole Network in February 2017.

The graph below demonstrates that the number of SARs received in 2013/14 was greater than in the following two years, this was mainly due to an issue with suspicious MoneyGram transactions through the China and Russia/Ukraine corridors that year.

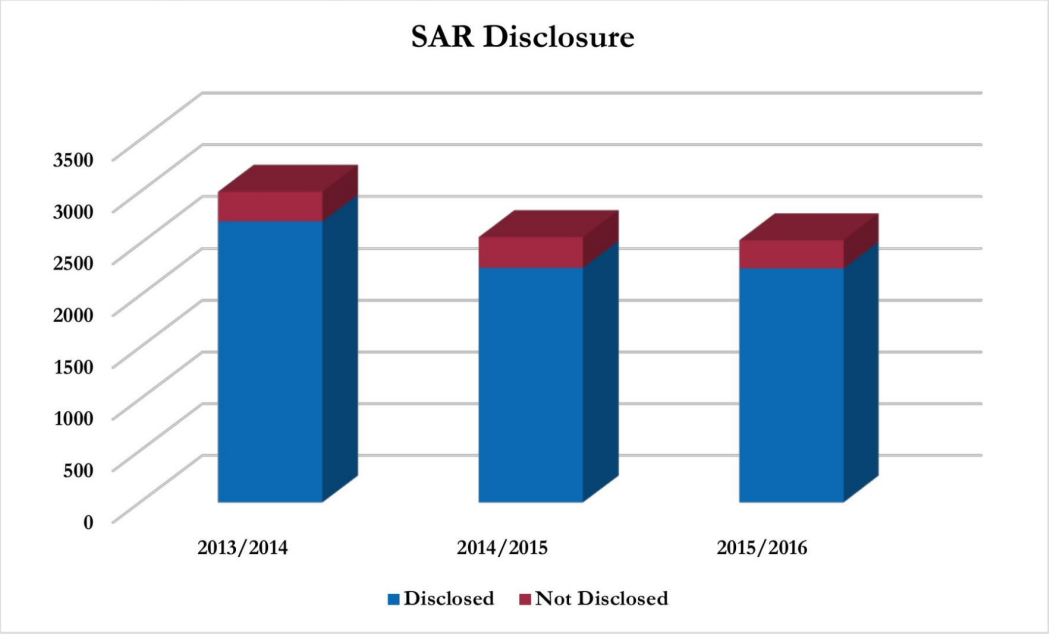


In October 2015, Post Office started to accept card payments for MoneyGram and as a result has seen an increase in suspicious activity. This has led to a growing trend of card fraud and vulnerable customers falling victim to scams. In 2016/17 year-to-date (20/12/2016), a total of 2,370 SARs have been received. The number of SARs submitted is higher than previous years, with on average, c.260 SARs received per month. If the current run rate continues, by the end of 2016/17 the amount will exceed levels seen in the last 3 years.

The following graph shows the volume of SARs disclosed to the National Crime Agency (NCA). 2,261 SARs (89.26%) were disclosed to the National Crime Agency (NCA) in 2015/16, in comparison to 2,268 SARs (88.49%) in 2014/15. Additional training has been received from NCA, who have also given specific feedback to the team responsible

POL00247018

for disclosing SARs, so the overall growth in disclosure rates does not represent a more defensive approach to reporting.



All non-disclosed SARs and a sample of disclosed SARs are checked by the Head of Financial Crime each month.

POL00247018

5. Annual Risk Review: Legal

Author: Ben Foat Sponsor: Jane MacLeod Meeting date: 30 January 2017

Executive Summary

Context

The ARC annual planner states that the Committee will receive an annual risk review report on Legal risks each year. This paper provides the Committee with an update on the key Legal risks identified, their performance and what this means for our control environment.

Questions this paper addresses

- What are the key Legal risks?
- What governance and assurance is in place to control these risks?
- What is the overall position and further actions required?

Conclusion

1. The Post Office risk appetite is ***averse*** for non-compliance with law and regulations or deviation from its business conduct standards.

   There is no specific risk appetite statement that covers contractual risk, however the following statements are relevant:
   - ***Averse*** appetite for risk taking which would alienate or lose significant groups of profitable customers;
   - ***Tolerant*** risk appetite for Legal and Regulatory risk in those limited circumstances where there are significant conflicting imperatives between conformance and commercial practicality.

2. In the view of the Group Legal Director the main areas of concern are:
   - Contract management experience and expertise must be seen as a core competency of Post Office. Significant improvements have been introduced over the last 18 months to assist the business to manage contracts compliantly, such as the provision of contract and PCR training, refinement and enforcement of the CAF process, development of a Material Contracts Register, and Contractual Obligations Spreadsheet. Nevertheless there is still significant room for improvement; for example the legal team is aware of contracts having expired while services are still being provided; services being provided or received from third parties without appropriate written contracts in place, and contracts being breached because the obligations imposed are not either understood or monitored. More work is being carried out to assist the business to act compliantly in this regard including the development of a central repository of all contracts through the existing Bravo system, further refinement and enforcement of the CAF process, contract standardisation, and further training to the business.
   - There are numerous contracts, property documents or other documents with legal consequences, which are not readily available within the business. This increases the risk of non-compliance as well as the inability to properly manage the contract or for Post Office to comply with its own obligations. The development of a central repository for all contracts together with the standardisation of contracts will reduce this risk going forward.

POL00247018

- There is a lack of understanding across the business of the relevant regulatory obligations. Regulatory knowledge is dependent on a few core individuals. There is also a lack of internal knowledge around Post Office regulatory obligations in circumstances where we have outsourced activity but not accountability. The Legal Team has developed a Regulatory Matrix Register so that the business can better understand these obligations and proactively manages changes to the regulatory environment. Going forward, the establishment of new Compliance Team will assist in reducing this risk together with further training to the business.
- Many of Post Office's activities need to be considered in light of competition rules, and there needs to be better understanding of the potential implications of commercial activities such as joint ventures and even information sharing arrangements. Monitoring of and compliance with the 'Restrictions policy' operated by Post Office and embedded in agents' contracts needs to be carefully considered. The Legal Team is finalising Competition Guidance which will be rolled out across the business.
- While Post Office has a prosecutions Policy, the number of incidents of Post Office bringing prosecutions itself has decreased dramatically and there have been no prosecutions brought by Post Office to date in 2016-17. The risk is that any deterrent effect of such prosecutions has been eroded and opportunistic behaviours by agents may be increasing.
- Project Sparrow is not within the scope of this report. A separate verbal briefing will be provided to the Board.

3. Further detail of these risks are set out in the Report and in Appendix 1, together with a high level summary of the current controls in place to mitigate against these risks and the further work that is underway to improve these mitigations.

4. The Legal Team has drafted a Legal Policy and established the Legal Risk Register. Further work is required to collate meaningful data on these risks. Within that framework, the Legal Team mandates the approval and execution of legal documents in accordance with the Board approved delegations of authority (overseen by Corporate Secretariat); a legal Risk Report is provided in respect of all new material contracts; legal risks are included in the Risk logs for projects; legal and regulatory risks are monitored by the General Counsel through the Post Office risk universe and risk registers; and potential risks arising from upcoming legal and regulatory developments are flagged to the RCC and the ARC through the Horizon Scanning report.

5. The most recent assurance activity undertaken on specifically legal risks was the Contract Management Audit undertaken in 2015. There have been a number of audit and assurance reports on regulated activities – particularly in relation to the set up and early operations of POMS; and both Bank of Ireland and POMS undertake regular assurance on aspects of Post Office's regulatory activities.

Input Sought

The Committee is asked to note this reportand endorse current actions designed to mitigate these risk.

POL00247018

The Report

What specific risks should the Committee be aware of?

Contract Management and Procurement Risk

6. As the Committee is aware, deficiencies with the contract management and procurement processes were identified following an internal audit report in 2015. While the actions identified in that audit have been addressed, there remains further work to enforce a compliant culture – both by the legal and procurement teams, but also by wider Post Office management.

7. There is further work to be done in relation to contracting processes, improving understanding of the contractual obligations imposed by contracts and developing experience and expertise of how to manage contracts, understanding of the impact of contracts on other areas within the business, as well as improving knowledge of basic contract law and the Public Contract Regulations 2015 ('PCR') to which Post Office is subject.

Loss of legal documents

8. Connected to Contract Management and Procurement Risk identified above is the loss of legal documents. There are numerous contracts, property documents or other documents with legal consequences, which are not readily available within the business. Consequently, there is a real risk of failure to properly manage those contracts but also potentially giving rise to non-compliance with regulatory requirements and principles. This could result in brand damage, financial loss or regulatory censure.

9. **Further Actions:** Steps have already been taken to develop and improve controls, and further work remains to be done. In particular:

- the previous CAF process (which only applied to 'material' contracts) was re-designed and is in the process of being extended so that all documents creating or varying legal obligations must go through a consistent approval process under which the contract owner certifies that the contract is appropriate for Post Office to enter into; authority to execute contracts is limited to identified roles and/or named individuals;
- a contracts database has been developed so that among other data, an electronic copy is kept of the signed version of all contracts entered into by Post Office; we are currently in the process of adding the backlog of over 1000 contracts to the database, however we believe there are likely to be more contracts of which we have no formal records.
- development of the Contract Obligations Spread sheet which to date has been applied to the 'Top 25' contracts, and which going forward will be applied to all material contracts from execution;
- the provision of a number of training sessions on basic contract law, procurement law, and contract management to those involved in the procurement processes and contract management;
- membership of the IACCM and provision of e-learning training through that program to a pilot group of contract managers;

POL00247018

- in conjunction with the procurement team, development of procurement manuals etc to provide guidance on common issues;
- development of Post Office 'house positions' and standardised drafting on specific issues so as to facilitate negotiations;
- development of standardised legal risk reports in relation to new contracts to better describe the risks associated with specific contracts and agreed mitigations and actions.

Non compliance with regulatory requirements and principles

10. Post Office is a multiline business subject to a number of regulatory requirements and regulators. The key regulators relevant to Post Office include:

HMRC	AML in relation to regulated products and services
ICO	Data Protection (issues involving the use of personal data) and Freedom of Information;
CMA	Competition (anti-trust);
OFCOM	Telecommunications and mails;
FCA	Regulated financial services (most relevant to POMS), but also regulates competition in financial services, consumer credit and payments services (in its dual capacity as Payment Services Regulator)

11. In addition, Post Office is indirectly subject to regulatory requirements which flow down through its Appointed Representative status with each of Bank of Ireland and POMS under the contractual arrangements with each of them as regulated entities.

12. Other contractually imposed regulatory requirements include those imposed by the UK Banking Industry in respect of the Banking Services it offers to customers (i.e the deposit and withdrawal of cash at branches), compliance with various mails regulations eg Dangerous Goods, and telecom regulations.

13. Although there is little direct regulation of Post Office by these Regulators, there remains a lack of understanding across the business of the relevant regulatory obligations which is confined to a limited number of key individuals in each area and there would be a material lack of knowledge should these individuals leave. There is also limited oversight of Post Office regulatory obligations in circumstances where we have outsourced activity but not accountability.

14. **Further actions:** The General Counsel is in the process of establishing a new Compliance function, and once established this will help to coordinate a wider view of the regulatory framework within which Post Office operates, a greater understanding of the cross-dependencies and implications of Post Office's various activities, and a coordinated approach to the management of regulatory risks including any response to regulators. As Financial Services becomes an increasingly important part of Post Office's future growth, the development and embedding of a compliant culture will be critical.

15. Further training is to be provided to the business through next year including, for example, on the impact of the Senior Manager's Regime and General Data Protection Regulations.

POL00247018

16. Legal has developed a Regulatory Matrix Register, which defines the breath of regulatory requirements on Post Office and identifies the relevant regulator. Various policies have been established to manage these risks (AML, ABC) etc. The Legal Department also uses a regulatory development trackers to update the business on changes to the legislative and regulatory landscape which are reported to the RCC and ARC through the Horizon Scanning report.

Competition Law

17. There are a number of areas of Post Office's activities where competition law issues can and do arise. These include:

    - When contracting, Post Office needs to be careful not to include restrictions/benefits which could be deemed to be anti-competitive (certain exclusivities, pricing structures, terms which limit supply/production in a particular market etc.); Activities undertaken as part of our relationship with Royal Mail also need to be carefully considered from a competition perspective.
    - As a sub-set of the above, Post Office's restrictions clause in its contracts with agents needs to be kept under review;
    - When holding exploratory talks with potential partners (JVs, acquisitions etc.);
    - When participating in industry wide associations; and
    - During procurement exercises - both where Post Office is bidding/involved as a bidder (e.g. in response to government and utility contracts) and where Post Office is itself procuring goods/services.

18. The Post Office legal team includes competition law expertise and our commercial lawyers have a good understanding of basic competition law issues so that potential competition concerns can be identified early and appropriately addressed.

19. Restrictions clauses in contracts with agents are regularly monitored and discussed with the Post Office Restrictions Manager, Paul F Williams, to understand developments in monitoring compliance with this clause across the agency network and how these restrictions may be compliantly enforced. There have been challenges to Post Office's approach previously and Post Office has previously argued successfully that the restrictions policy is needed to maintain the network (as we did, successfully, before the European Commission in relation to Post Office 2015-2018 state aid).

20. One key area of potential risk, is information sharing between Post Office and third parties. On projects, Post Office has a precedent Information Sharing Protocol (distinct from the standard form NDA) which is signed by all parties to the proposed deal to ensure that key staff/contractors on both sides are aware of competition law and their obligations thereunder.

21. The Legal Department has arranged and will continue to give competition law training to different areas of the business and project teams to ensure that competition law issues are highlighted early and dealt with appropriately. Aside from the recent "Choice" competition law litigation concerning Supply Chain - an area of the business which has received support from external competition lawyers over the past year - there have been no major incidents in relation to competition law in the past year.

POL00247018

22. **Further Actions:** The legal function is drafting a Competition Guidance to increase awareness of competition law issues across the business, and further Competition law training will continue to be rolled out across more business units to ensure there is greater appreciation of the legal risk, and when to raise competition law issues with Post Office Legal.

Dispute Resolution Management

23. Historically Post Office has had relatively few incidents of material litigation arising from commercial or contractual disputes– given the concerns expressed earlier as to Post Office's historic lack of understanding and enforcement of its legal rights, this seems unusually fortuitous. As Post Office seeks to become more commercially independent, there will be a greater emphasis on the need to manage disputes carefully.

Prosecutions

24. **Further actions:** Over the last few years Post Office has undertaken very few prosecutions by contract to its previous practices – none have been brought to date in 2016-17. This lack of appetite has been observed by the agency network. It remains to be seen whether the reduction in prosecutions will directly result in higher incidences of opportunistic behaviours, however agent losses are increasing.

25. Post Office has a Conduct of Criminal Investigation Policy which sets out the procedure to manage Prosecutions. Work being undertaken as part of the defence of the current action brought by Freeths on behalf of c 200 post masters, should assist Post Office to have greater certainty of success should it re-commence prosecutions.

26. The Legal Department is in the process of drafting Dispute Resolution and Brand Protection Manuals to better understand the array of dispute resolution and enforcement risks as well as gathering MI data on the number of disputes that Post Office is involved in. Once that data is available, Post Office will be better placed to understand the types of risk and employ more effective controls to mitigate against those risks.

POL00247018

Appendix 1: Summary of Post Office Legal Risks (not including Financial Crime or Information Security)

Key Legal Risks	Performance of Risks	Governance & Assurance (Controls)	Overall Assessment	Further Actions
Contractual Management and Procurement Risks	There is a lack of understanding of how to manage contracts; the contractual obligations imposed on each party, impact to other areas within the business; basic contract law and PCR requirements.	CAF Process Material Contracts Register Top 25 Supplier Contractual Obligations Training to the business on basic contract law and contract management		CAF refinement Bravo Project (central repository of contracts) Legal Tracker
Loss of Legal Documents	There are numerous contracts, property documents or other documents with legal consequences, which are lost or are not readily available within the business. Consequently, there is a failure to properly manage those contracts but also potentially giving rise to non-compliance with regulatory requirements and principles.	Co Sec Safe Existing CAF process		Bravo Project (central repository of contracts) Refinement of CAF Process
Dispute Management (including Prosecutions)	PO has made operational or strategic errors when it manages disputes and these errors can lead to financial losses and significant additional project / management time to resolve. There is also a lack of enforcement by PO of its legal rights.	Conduct of Criminal Investigations Policy Training to business and Legal support		Dispute Resolution and Brand Protection Manual Legal Tracker MI
Non-Compliance with Regulatory Requirements and Principles (including Competition)	There is a lack of well defined regulatory requirements and understanding which could result in PO breaching its legal and contractual obligations. There is a lack of clarity of the full extent of regulatory oversight and interconnected requirements to other parts of the business that may not "own" the contract or service. There is also a lack of certainty around PO regulatory obligations in circumstances where we have outsourced activity but not responsibility.	Regulatory Matrix Regulatory Developments Tracker Training to the business Corporate policies Legal Dept. advisory support		Review of existing Corporate Policies Coordinated Forum for Financial Crime Training to business e.g SMR and GDPR

POL00247018

POST OFFICE LIMITED
AUDIT RISK & COMPLIANCE COMMITTEE

6) Internal Audit Report

Author: Johann Appel Sponsor: Jane MacLeod Meeting date: 30th January 2017

Executive Summary

Context

The purpose of this paper is to update the Committee on the PO Business As Usual Internal Audit (BAU) and Business Transformation Assurance (BTA) activity and key outcomes. This includes details of the work completed since the last Audit, Risk and Compliance Committee (ARC) in November and progress on the 2016/17 Internal Audit Plan, as well as progress on integrated assurance initiatives.

Questions this paper addresses

1. What progress has been made since the November meeting?
2. What key messages and themes are emerging from the reviews we have completed (BAU and BTA)?
3. Is the Internal Audit Plan on track? Do we have the resources we need to deliver the plan and actions arising?
4. Have any significant issues arisen that the committee should be aware of?

Conclusion

1. **Audits finalised and in progress:**

   Since the November ARC, four reviews have been completed and finalised:

   Business as Usual (BAU):

   (1) Data Protection
   (2) FS Training & Competence Scheme
   (3) Vetting

   Business Transformation Assurance (BTA)

   (4) Winning with Retailers PIR).

   One BAU review is nearing completion: FS Branch Network Sales Process.

2. **Key Messages and Themes:**

   We are collating the findings from all audit reviews completed in 2016 and have summarised them against the General Controls Framework (GCF) to identify common control themes across the business.

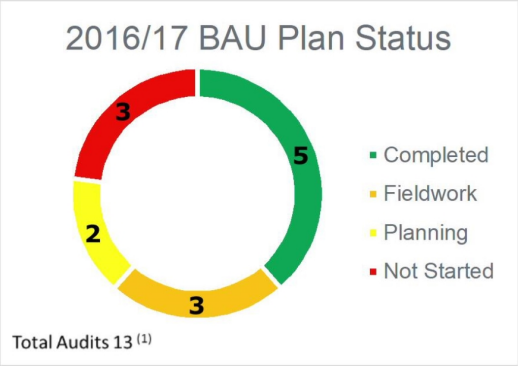
   The top 5 recurring themes (by number of findings and number of audits) can be summarised as follows (all these themes occurred on one or more audits presented in this report):

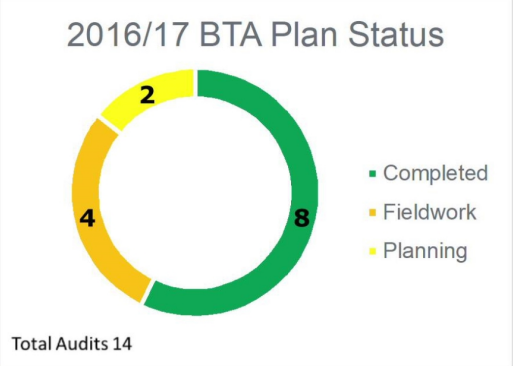
   (1) Incomplete or outdated documentation for operational processes, policies and controls.

POL00247018

(2) Unclear roles and responsibilities, including accountability for performing controls.
(3) High level of dependency on knowledge and expertise of key individuals and/or teams are not adequately resourced.
(4) Misalignment between development of new business solutions or systems and Post Office strategic directions. Strategic objectives, deliverables and future roadmap are not clear or well defined.
(5) Insufficient or inadequate MI in place for monitoring the performance of key controls or to identify potential risks and exceptions.

3. **Progress against plan:**
The BAU audit programme is currently behind as a result of slippage that occurred during the summer due to staffing issues. We are catching up and are confident that the audit plan will be delivered as planned by the May ARC. Two audits have been postponed and two management requests were added to plan. The remainder of the current year plan is being reviewed in context of the recently announced reorganisation and changing priorities. Delivery of the BTA audit programme is progressing as planned.





(1) Original plan 12 + 2 additions +1 carried forward from 2015-16 - 2 postponed

Full summaries of Audit Plan Status are included in **Appendix 1a and 1b**.

Audit Action Status:	**BAU**	**BTA**
Open (not yet due)	17	28
Overdue (< 30 days)	0	4(2)
Total	17	32

(2) There are 4 overdue actions from the Information Security Review. Management are aware that these actions are overdue, and revised mitigation dates have been put in place.

4. **Significant Issues:**
There are no significant issues we believe the committee should be made aware of at this time.

Input Sought

The Committee is asked to note and provide comment as necessary.

POL00247018

The Report

5 BAU Internal Audit Reviews - Completed

The three BAU audits finalised since the November ARC have reported good practices and/or progress in these key business processes. However, there were some control weaknesses identified that require corrective management action:

Audit	Key Messages
Data Protection *(Ref. 2015/16-05)* Average	• Data protection policy framework was incomplete or out of date and there was a lack of ownership and oversight over POL's Privacy Programme. • Impact of change programmes on personal data were not always considered and/or ISAG not adequate engaged. • Privacy risk for legacy processing activities has not been reviewed and prioritised. • Data protection awareness initiatives at branch level were insufficient.
FS – Branch Network Sales Training & Competence *(Ref. 2016/17-03)* Average	• Training & Competence (T&C) arrangements not in place for Counter Colleagues and Branch Managers who sell or introduce FS products or services (Action to implement appropriate and proportionate training procedures). • There is no robust mechanism to ensure that Counter Colleagues' knowledge is properly tested. • Insufficient Management Information (MI) to have proper oversight over the T&C Scheme.
Vetting *(Ref. 2016/17-09)* Average	• No vetting conducted for employees who joined prior to 2004. Vetting for 2004-2008 conducted by RMG with no records available, consequentially there POL will not be able to demonstrate that the originator of a regulated transaction is "fit and proper" to conduct that transaction. • Vetting records kept on different systems for Directly Managed and Agents staff and as a result are not readily accessible. • There is no ongoing vetting programme; instead employees are expected to self-declare any criminal charges or convictions that may impact their ability to originate regulated transactions.

Management have accepted these findings and corrective actions have been agreed. Executive summaries of the above three audits are attached as **Appendix 2a – 2c.**

6 BAU Internal Audit Reviews - In Progress

6.1 FS Branch Network Sales Process - on track

6.2 Identity and Access Management - on track

6.3 Financial Controls Framework (Independent Validation) – on track with Phase 1 (Client Settlements Process) complete and found that 100% of tested controls are designed and operating effectively.

A full summary of Audit Plan Status is included at **Appendix 1a**.

POL00247018

7 Business Transformation Assurance Reviews - Completed

During the period the Business Transformation Assurance team have completed one review, Winning with Retailers PIR. Key messages from this audit are:

Audit	Key Messages
Winning with Retailers PIR Not Rated (PIR)	• Lessons learned were not documented for the benefit of future change programmes. • No evidence of benefits management and tracking for the Network Development (ND) and Win in Mails (WIM) programmes. • Sub-optimal stakeholder engagement and management of partner relationships due to a lack of detailed feasibility assessments during Project Ivy pilot.

Lessons Learnt have been included in the current change methodology, One Best Way. An executive summary of the above audit is attached as **Appendix 3a.**

8 Business Transformation Assurance Reviews – In Progress

Four reviews are in progress (TOM Development, 3rd Party Vendor Management, Business Case Development, and Data Management & Quality).

A full summary of BTA Progress to Plan status is included as **Appendix 1b**.

9 Updates on Internal Audit Overdue Actions

9.1 **BAU Audit Actions:**
We reported three overdue actions to the November ARC. All of these actions have since been closed with 17 actions remaining open within their due date.

9.2 **BTA Audit Actions:**
There were no BTA action overdue at the time of the November ARC. There are currently 32 open actions, of which 4 actions from the Information Security review are now overdue (<30 days). Management are aware that these actions are overdue, and revised mitigation dates have been put in place. In addition, open audit actions for this review are now overseen and prioritised by the monthly Security Transformation Steering Group.

10 Updates on Integrated Assurance initiatives

10.1 **Assurance Map:** An Assurance Map is being populated to provide a holistic view of all assurance activities. The assurance map will also highlight any gaps in high risk areas, prevent duplication of effort and inform future audit planning.

10.2 **Control Self-Assessment (CSA):** Implementation of CSA is well advanced and 11 finance processes have gone live. PwC has been engaged to provide independent assurance over a sample of controls. Particular focus of testing is being given to reconciliations. Phase 1 (Client Settlements) was completed in December with 4 minor risk and control descriptions improvements recommended.

POL00247018

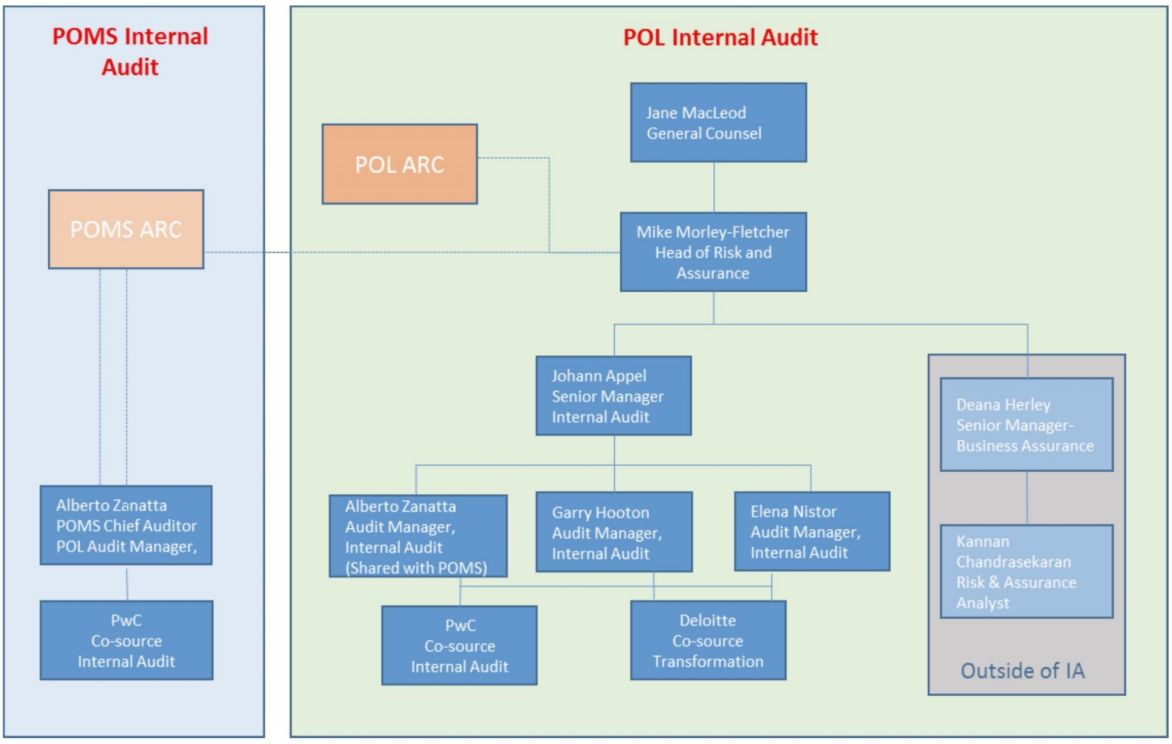
These have been accepted and will be actioned for the next CSA. Phase 2 (Bill to Cash, Project Accounting, Record to Report, Payroll and Tax) is now underway. Separately, 'HMRC Registration' key controls will be assessed using the CSA tool from February.

The CSA regime will be replicated to provide assurance over the IT Controls Framework that is currently being implemented.

10.3 **General Controls Framework:** The results of the current state assessment for general controls is being re-communicated and updated with new SME owners given the significant changes in accountabilities, ahead of final assessment by General Executive Control Owners, at year end.

11 Resourcing

For Internal Audit reviews we have a headcount of three managers and an Internal Audit senior manager, supplemented by approximately 150 days of co-sourced resource from PwC for specialised audit work. In addition we have co-source support from Deloitte for our Business Transformation Assurance (BTA) work. The Deloitte BTA support runs until March 2017 and the PwC co-source agreement until June 2017. We will be conducting a formal retender in due course (preparations have already started with the Procurement team). Following is the organisation structure for Internal Audit:



POL00247018

Appendix 1a

	POL- 2016/17 Plan						Actions			Reporting		
Ref.	Audit Title	Key Audit Contact	Timing	Revised Timing	Status	Report Rating	High	Medium	Low	Due RCC	Due ARC	Comments
1	IT Disaster Recovery and Resilience	A.Cameron (J.MacLeod)	Q2	Q3	Final (ARC)	Adverse [1]	3	5	0	03 November 2016	17 November 2016	Provided to RCC and ARC in November.
Addition to plan (Man request)	DC Pensions Issue	A. Cameron	Q2		Final (ARC)	Not rated				03 November 2016	17 November 2016	Provided to RCC and ARC in November.
21 (from FY15/16 plan)	Data Protection	J. MacLeod	Q2	Q3	Final (GE)	Average	0	8	2	10 January 2017	30 January 2017	
2	FS Training and Competence schemes - PO Network	N. Kennett (K. Gilliland)	Q1		Final (GE)	Average	1	9	15	10 January 2017	30 January 2017	
Addition to plan (Man request)	Vetting	J. MacLeod	Q3		Final (GE)	Average (TBC)	0	3	0	Report circulated via email to RCC prior to ARC	30 January 2017	
3	Identity and Access Management (Joiners, Movers, Leavers)	A. Cameron (M. Kirke)	Q2	Q4	Fieldwork					09 March 2017	27 March 2017	ToR reviewed and updated due to change of scope after initial planning with CFO. Audit delayed as audit manager was away (maternity leave).
4	FS Branch Network Sales Process Review	N. Kennett (K. Gilliland)	Q3		Fieldwork					09 March 2017	27 March 2017	Unable to complete site visits in December due to operational reasons. RCC and ARC reporting postponed from Jan to March.
5	Branch Audit (revisit and update)	K. Gilliland	Q3	Q4	Planning					09 March 2017	27 March 2017	Delayed due to the vetting audit (management request). Planning / Scoping phase revisisted following re-organisation.
6	Financial Controls Framework Programme - Independent Testing	A. Cameron	Q3/Q4		Fieldwork					04 May 2017	18 May 2017	Audit to be completed over 4 phases. PwC co-source arrangement.
7	Network Branch Service Centre - Handling of Agents Queries and Complaints	K. Gilliland (A. Cameron)	Q3	Q4	Not started					04 May 2017	18 May 2017	
8	IT & Operations Governance and IT Risk Management	R. Houghton	Q3	Q4	Not started					04 May 2017	18 May 2017	Approach to this audit being discussed with CIO - Potentially to be combined with 9
9	IT Third Party Management	R. Houghton	Q4		Not started					04 May 2017	18 May 2017	Approach to this audit being discussed with CIO - Potentially to be combined with 8
10	FS Sales Operations -1st Line of Defence	N. Kennett	Q4		Planning					04 May 2017	18 May 2017	
11	Procurement Process	A. Cameron	Q4	2017/18	Postponed					FY 2017/18	FY 2017/18	New Head of Procurement currenlty reviewing processes. Postpone the review to 2017/18.
12	Business Continuity and Crisis Management - PO	K.Gilliland (J. MacLeod)	Q3	2017/18	Postponed					FY 2017/18	FY 2017/18	Suggest this is one of the postponed audits - to make way for DC Pensions / Vetting.

[1] Following further review and discussion with the CIO (Rob Houghton) it was agreed to update the rating for the IT DR report from Average to Adverse

POL00247018

Appendix 1b

	BTA- 2016/17 Plan						Actions			Reporting		
No.	Audit Title	Key Audit Contact	Timing	Revised Timing	Status	Report Rating	High	Medium	Low	Due RCC	Due ARC	Comments
1	End to end Financial management of Transformation	D.Hussey	Q4	Q1	Final (ARC)	Average	1	8	5	05 May 2016	19 May 2016	
2	Portfolio Management OE#1	D.Hussey	Q4	Q1	Final (ARC)	Satisfactory	0	1	2	05 May 2016	19 May 2016	
3	Digital Programme Mobilisation	M.George	Q1		Final (ARC)	Adverse	6	1	0	14 July 2016	28 September 2016	
4	Planning Boot Camps #2	D.Hussey	Q1		Highlight Report	Satisfactory	1	9	15	14 July 2016	28 September 2016	
5	Communications and Stakeholder Management	D.Hussey	Q1	Q2	Final (ARC)	Satisfactory	0	2	1	14 July 2016	28 September 2016	
6	IT Separation (From RMG)	A. Cameron	Q3	Q3	Final (ARC)	Not Rated (PIR)	6	5	1	03 November 2016	17 November 2016	
7	Information Security	J.MacLeod	Q3	Q3	Final (ARC)	Adverse	8	3	6	03 November 2016	17 November 2016	
8	Winning with Retailers	M.George	Q1	Q2	Final (RCC)	Not Rated (PIR)				10 January 2017	30 January 2017	
9	Target Operating Model	D.Hussey *	Q2	Q4	In progress-Fieldwork					09 March 2017	27 March 2017	Work suspended pending TOM Board Paper submission - Nov 16. Work scheduled to recommence January 2017
10	Data Management and Quality	J.MacLeod	Q3	Q4	In progress-Fieldwork					09 March 2017	27 March 2017	Terms of reference being discussed with sponsors
11	3rd Party Vendor Management	A. Cameron	Q3	Q4	In progress-Fieldwork					09 March 2017	27 March 2017	Terms of reference being discussed with sponsors
12	Project Expenditure Approval Process	J.MacLeod	Q4		Scoping					09 March 2017	27 March 2017	An additional audit following a request from management
13	Business Case Development	D.Hussey */ A.Cameron	Q4		In progress-Fieldwork					04 May 2017	18 May 2017	Scoping
14	Ox Blood' Red rated risk reviews	D.Hussey */ A.Cameron	Q4		Scoping					04 May 2017	18 May 2017	Scoping
On hold	Support Services Transformation	A.Cameron	Q3	Q4	On Hold							
On hold	POCA	N.Kennett	Q3		On Hold							Project on hold until Banking partner signed up - Assurance work consequently on hold.
Cancelled	Back Office Tower Transition	A. Cameron	Q3		Cancelled							Postponed indefinitely

* Ownership to be determined.

POL00247018

Appendix 2a

INTERNAL AUDIT EXECUTIVE SUMMARY: Data Protection

Ref. 2015/16-05

GE Sponsor: Jane MacLeod, Legal Counsel

Average

1. Background

The UK Data Protection Act (DPA) 1998, requires organisations to implement and operate appropriate controls to manage and protect personal data of employees and customers. As one of the workstreams to obtain assurance over Post Office Limited's (POL) compliance with the UK Data Protection Act (DPA) 1998, an audit has been undertaken to assess POL's operational privacy controls. In addition Post Office will be reviewing its controls and processing relating to the upcoming European General Data Protection Regulation (GDPR) requirements.

2. Audit Objective and Scope

The objective of this review was to assess POL's data protection controls and governance to comply with the UK Data Protection Act 1998. The scope of this audit included:

- A review of data policies and procedures to ensure they are fit for purpose and effectively deployed and communicated within the business.
- Third party data processing policies.
- Roles and responsibilities of data owners and data chief officer.
- Effectiveness of the data incidents process.
- Data requirements for new projects are data specialist involvement in new projects.
- Data protection training.
- Data locations identification and data access management.
- Data transfer and security controls in place when transferring data.

3. Key Observations

This audit identified eight moderate findings. Key audit observations were:

- Data protection policy framework (standards, policies and procedures) was incomplete or out of date and policy documents were not owned by the Information Security Assurance Group (ISAG).
- The impact of change programmes on personal data and consequential obligation to comply with the Data Protection Act 1998, were not always considered and/or the Information Security Assurance Group (ISAG) were not adequately engaged.
- POL has not conducted a review of its legacy processing activities, to prioritise those that it believes present the greatest level of privacy risk.
- There is a lack of ownership and oversight over POL's Privacy Programme.
- Data protection awareness initiatives at branch level were insufficient. Furthermore there was inadequate notification to data subjects as to the nature of data collection and processing thereof.

POL00247018

Appendix 2a

INTERNAL AUDIT EXECUTIVE SUMMARY: Data Protection

Ref. 2015/16-05

4. Conclusion

We have rated this report **Average** due to some weaknesses in internal controls which need resolving immediately.

The majority of the control weaknesses relate to the theme of management and oversight of POL's privacy programme. Under the DPA 1998, the requirement for appropriate controls for privacy programme management is an implicit requirement of good governance. Under the current regime the risk of non-compliance may not have a material impact, however, the upcoming EU GDPR will have more explicit requirements and will require active demonstration of compliance.

The General Data Protection Regulation project to be initiated shortly will focus on personal data and how this is owned, used, managed and protected, in reference to compliance with the future requirements of the GDPR 2018.

5. Management Response

"We concur with the audit findings and have agreed to take action to improve the controls over the management and protection of personal data."

- Jane MacLeod (General Counsel)

POL00247018

Appendix 2b

INTERNAL AUDIT EXECUTIVE SUMMARY: Financial Services – Branch Network Sales Training & Competence Review

Ref. 2016/17-03

GE Sponsors:
Kevin Gilliland, Network and Sales Director
Nick Kennett, Director of Financial Services

Average

1. Background

As an Appointed Representative (AR) of the Bank of Ireland (UK) Plc (BoI) and Post Office Management Services Limited (POMS), the Post Office Limited (POL) has a regulatory responsibility and contractual obligations to put in place effective systems and controls by which staff involved in POL's financial services business receive appropriate training and oversight.

2. Audit Objective and Scope

This review assessed the adequacy and effectiveness of POL's training and oversight arrangements to ensure that staff introducing and selling financial products and services, within the branch network (both Directly managed and Agency) are appropriately trained and competent to support the product range made available to consumers. This review was not designed to assess the compliance and product training modules. The scope of this audit included:

- Training & competence (T&C) frameworks - Assess the existence and adequacy of the T&C frameworks, including qualification requirements (as appropriate) to meet regulatory expectations for the Financial Specialists (FSs), Mortgage Specialists (MSs), hybrid FSs/MSs, Customer Relationship Managers (CRMs) and counter staff within the branch network.
- Training & competence (T&C) management information (MI) - Assess how POL monitors the training and competence of the sales staff in delivering fair consumer outcomes.

3. Key Observations

This audit identified 1 high and 9 medium findings. Key audit observations were:

- ***There are currently no Training & Competence (T&C) arrangements for Counter Colleagues and Branch Managers*** involved in the introduction and / or selling of financial products and services, across either the Directly Managed or Agency Branch Network. There is a risk of insufficient or inaccurate information being provided to customers and / or mis-selling. As a comprehensive training framework was not deemed feasible, management agreed to implement a training regime that is appropriate and proportionate to the risk.
- ***There is no robust mechanism to ensure that Counter Colleagues' knowledge is properly tested.*** The system used (Horizon) to test the compliance knowledge of Counter Colleagues allows individuals to undertake unlimited test attempts and does not have the ability to capture failed attempts. Staff having difficulty in answering questions, ask for assistance from their Branch Manager or colleagues to correctly answer the test question. Furthermore, Counter Colleagues' product knowledge is tested on a group basis following Capability Matters training. There is a risk that individual coaching or development needs are not identified and addressed.
- ***Insufficient Management Information (MI) to permit proper oversight over the T&C Scheme.*** The MI reporting for the Scheme did not include information that

POL00247018

Appendix 2b

INTERNAL AUDIT EXECUTIVE SUMMARY: Financial Services – Branch Network Sales Training & Competence Review

Ref. 2016/17-03

we typically expect to see in order to monitor delivery of the various requirements of the Scheme, such as: the spans of control for Supervisors; the competence status of staff that operate within the Scheme; the length of time taken to achieve accreditation under the Scheme; the number and reasons for exceptions raised in relation to achieving accreditation; and results of POM Academy testing (including trends on areas of weakness or further development). Also, the commentary in the report does not analyse what is behind the data, it only describes what had occurred. Without such information, there is a risk that POL may not have sufficient oversight of the delivery of the Scheme to ensure that customers are being treated fairly.

- ***Untrained and non-competent staff*** - Management should ensure that branches not permitted to introduce or complete the sale of Financial Services products (i.e. Local branches) clearly understand the scope of their role especially as these individuals are not subject to any T&C arrangements. Whilst "Local" branches did not have the ability to complete financial services sales in branch via the Horizon system and did not stock financial services product leaflets, our visit to one Sub-postmaster Local branch identified that the branch had obtained a limited selection of leaflets (which appeared to be out of date). This presents a risk that insufficient or inaccurate information is provided to customers and / or possible mis-selling.

4. Conclusion

POL has two core training and competence arrangements in place: the T&C Scheme ("the Scheme"), designed for Financial and Mortgage specialists and the T&D Framework ("the Framework"), designed for Customer Relationship Managers (CRMS). Both the Scheme and the Framework have practical toolkits to support individual development and the maintenance of formal record keeping arrangements. The Scheme and the Framework appear to be operating as currently designed.

The new training system ("Success Factors") will bring all the training into one system and will allow for better monitoring, oversight and reporting of training completed by counter colleagues. This will be in place by July 2017.

We have rated this report Average as we identified some weaknesses in internal controls which need resolving, specifically around the breadth of POL's training and competence arrangements, as well as the gaps identified in the design of the Scheme and Framework and in the management information used to monitor the delivery of the various requirements.

5. Management Response

"This was a thorough and comprehensive audit. We agreed on the actions being recommended.

A project has been kicked off (and it is planned to be completed by July 2017) to ensure that all users across the Network receives the relevant training. Completion of trainings will be monitored and users will be prevented from processing a sales until they have completed the required tests. The development of the Success Factor delivery platform will allow trainings to be provided across the Network and their completion to be tracked. The roll out of the Enhance User Management (EUM) system will allow assigning a unique identifier to each users and allow relevant people to receive the training they needed and prevent them from processing any transactions until the relevant trainings are taken and tests passed."

- Owen Woodley (Sales Director)
- Jonathan Hill (Head of Financial Services Risk, Governance)

POL00247018

Appendix 2c

INTERNAL AUDIT EXECUTIVE SUMMARY: Vetting

Ref. 2016/17-09

GE Sponsors:
Jane MacLeod, General Counsel
Nick Kennett, Director of Financial Services

Average

1. Background

Under the terms of various client contracts and in accordance with regulatory requirements (including PO's role as Authorised Representative (AR) for Bank of Ireland (BoI) and Post Office Managed Services (POMS) and SYSC8, Post Office is required to ensure its staff, agents and agents' employees are properly qualified and appropriately vetted. In some cases clients have a right to audit compliance with this requirement. Recent audit and compliance reports have found issues with vetting, training processes and record keeping.

2. Audit Objective and Scope

The objective of this audit was to evaluate Post Office's ability to demonstrate that its staff, agents and agent's employees are properly qualified and trained. The scope of this audit included:

- Understand the process for on-boarding our staff, agents and agents' employees, and how changes to circumstances (e.g. CCJ, bankruptcy, etc.) are managed.
- Select a sample of our staff, agents and agents' employees (via their IDs) on the Horizon system and ensure that they have been on-boarded correctly.

3. Key Observations

This audit identified 3 medium priority findings. Key audit observations were:

- ***Incomplete vetting of long serving employees:*** Staff employed (across all branch types) before 2004 were not subject to any vetting, while staff employed in Directly Managed branches between 2004 and 2008 were vetted by RMG (Sheffield), but Post Office have no access to these records.
- ***Vetting records for employees are not readily accessible:*** Vetting records are kept on separate systems and are managed differently for Directly Managed employees and Agents. Vetting records for Directly Managed colleagues are retained on the IRIS system in employee order, however, they are not identifiable by Branch.
- ***No ongoing vetting programme:*** Staff are only vetted on employment, there is no rolling programme to update vetting. Staff are expected to self-declare any criminal charges or convictions.

4. Conclusion

We rated this report Average as some historical weaknesses were identified in internal controls, which need to be addressed. Management are taking action to address the audit findings.

Controls over the vetting of employees that commenced post 2008 are standardised and generally operating effectively.

POL00247018

Appendix 3a

INTERNAL AUDIT EXECUTIVE SUMMARY:

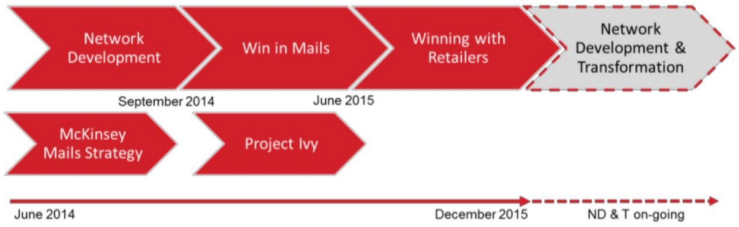
BTA - Winning with Retailers PIR

GE Sponsor: Martin George, Commercial Director

Not Rated (PIR)

1. Background

Winning with Retailers (WWR) was the culmination of a series of successive programmes that followed on from Network Development (ND) and Win in Mails (WIM), as well as related initiatives McKinsey Mails strategy and Project Ivy. These programmes spanned the period June 2014 to December 2015 (lifecycle depicted below).



Each programme had its own scope and set of deliverables, but they had a similar aim of creating a proposition for partners and retailers to provide a means to sell Post Office products and Services that would be more attractive than those of the leading competitors, and therefore defending and increasing market share in this area. The total spend on WWR was £3.1m, against an approved budget of £6.1m. Overall spend across all three programmes was c. £8.8m.

Due to issues with IT in the design phase and a lack of agreement on what the final proposition should look like, the WWR programme steering committee recommended that the scope be moved into the Front Office programme and subsequently the programme was closed at the design stage in December 2015, three months earlier than planned.

Some components of the WWR programme were transferred to other change programmes, i.e. the transition and delivery of the Access Points Model was transferred into the Network Transformation (NT) programme, and the associated technology of Access Points into the Front Office programme (now Branch Technology Transformation (BTT)).

2. Audit Objective and Scope

The objective of this post implementation review (PIR) was to help Post Office understand the reasons for closure of the programme and identify lessons to learn for benefit of future programmes.

The review assessed the following areas:

- The total spend and return of the current and previous iterations of the programme to date (1 moderate finding);
- Realisation of forecast benefits per the business case (1 major finding);
- Risks and issues associated with the programme, and how they were managed throughout the lifecycle (1 major and 1 moderate finding); and
- Governance, controls and reporting over key management decisions during the programme lifecycle and the reasons behind these, including management's rationale for premature closure of the programme (2 major and 1 moderate finding).

POL00247018

Appendix 3a

INTERNAL AUDIT EXECUTIVE SUMMARY:

BTA - Winning with Retailers PIR

3. Key Observations

It is noted that although the programmes were in progress before the implementation of One Best Way (OBW) change methodology, they were managed and governed using robust programme principles, such as Change Request processes, risk and issue management, and regular reporting to governance forums.

This review raised seven findings; four major and three moderate, all of which were translated into lessons learned. It is important that these lessons are considered and addressed both broadly across future PO programmes and specifically within the Network Transformation programme currently at business case approval stage (a follow-on project to WWR).

The four most important lessons learnt (related to the major audit findings) are:

1. There have been ***no lessons learned documented*** following the closure of any of these programmes. An interim programme closure report for WWR stated that a lessons learned document would be finalised in January 2016; however, this document was never produced. In mitigation the programme leadership and team remained the same between WIM and WWR and lessons learnt will be included going forward.
2. There was ***no evidence of benefits management and tracking*** for the ND and WIM programmes. There was also no evidence of benefits management and tracking within the WWR programme; however, this would have been of limited value since the programme was closed at the end of the design phase. It is important that all relevant benefits are carried forward into the Network Development and Transformation programme business case.
3. There was potentially ***sub-optimal stakeholder engagement and management of partner relationships***. A lack of detailed feasibility assessments during Project Ivy pilot may have had a detrimental impact on the reputation of POL amongst the partner retailers. Furthermore the early closure of a number of programmes initiated to develop propositions with key partners could potentially adversely impact POL's reputation, unless POL works closely with key stakeholders to manage these relationships.
4. Governance: There was ***insufficient document retention*** and subsequently business cases for the McKinsey Mails Strategy and Project Ivy were unavailable for this review. This issue was exacerbated by key programme personnel leaving the business before and during the review.

4. Conclusion

We have not rated this report due to it being a post implementation review of a programme that is already closed. The implementation of 'One Best Way' change methodology, if followed correctly will accomplish lessons 1 to 3, while the development of an Artefact and Document retention policy (currently being worked on) will address lesson 4. We concur with management that these actions will help to embed the lessons learnt for the benefit of future change programmes. The findings from this report are consistent with control themes reported previously in the past 12 months.

5. Management Response

"I am confident these lessons will be learnt through use of the One Best Way change methodology and robust monitoring by GE colleagues."

- Martin George (Commercial Director)

POL00247018

8) Risk Update

Author: Mike Morley-Fletcher Sponsor: Jane MacLeod Meeting date: 30 January 2017

Executive Summary

Context

The Central Risk Team has supported GE members in reviewing and reporting key risks and key further action, developing a risk & control environment "place mat" and considering their approach to risk appetite.

Questions this paper addresses

- What changes have there been to our **Key Risks**? What is the impact on our overall risk profile? What are the key "risks of the moment" to focus on?
- What have been the most significant **risk incidents** and **risk exceptions**? Do these change our view of the Key Risks?
- How are we planning for Management to manage our **risk and control environment** and ARC to monitor?
- What have we done with/ our plans for revising our **Risk Appetite Statement**?

Conclusion

1. Since September changes to the **Group Risk Profile** have included 1 new risk (6 IT Delivery Capability), 2 risks with increases in their net evaluation (5 Change Portfolio Delivery, 7 Transformation Resourcing – Payroll Legislation) and 5 with decreases. Overall our risk profile appears to have decreased following completion of KFAs as (a net of) four red risks have reduced to amber. There are 8 Key Risks that have been noted by Risk Owners as "risks of the moment" having potential to impact us over the next quarter and - these are receiving particular attention from Risk Owners. See appetite 1 for more details.

2. Our processes for, and management's awareness of, reporting **risk incidents** and recording **risk exceptions** are improving. Recent events do not suggest any changes to our view of the Key Risks or our Risk Appetite Statement.

3. Upon suggestion from the Chair of ARC the Central Risk team will develop a tool to facilitate discussion of the **Risk & Control Environment** and enable each business area to provide a snapshot self-assessment of their control environment for key risks. The tool will be trialled in Supply Chain, with results reported to the RCC and ARC in May.

4. We have reviewed the previous **Risk Appetite Summary** (Jan 2015) with GE Risk Owners and benchmarked against other organisation's statements. We will now test it in a RCC working session using a series of scenarios, based on real life

POL00247018

decisions already taken or to be taken, to validate the statements before presenting to ARC.

Input Sought

5. The Committee is asked to consider the proposed changes to our risk profile and the effectiveness of the proposed Key Further Actions to manage these risks, including the impact of recent risk incidents, and suggest any further changes.

POL00247018

Details

6. **Changes to the Group Risk Profile** since September are shown in red font (see appendix 1, tab 1), black solid arrows on the Heat Map and red font on the Key Further Actions (see appendix 1, tab 2). These include the following:

   - 1 new risks (6 IT Delivery Capability)
   - 2 changes to risk titles and descriptions (5 Change Portfolio Delivery, 7 Transformation Resourcing – Payroll Legislation)
   - 2 risks with increases in their net evaluation (5 Change Portfolio Delivery, 7 Transformation Resourcing – Payroll Legislation) as the next phase of Transformation becomes more complex and forthcoming legislation impacts our contractor resource.
   - 5 risks with decreases in their net evaluation (16 Industrial Relations, 20 Transformation Benefit Realisation, 23 Financial Reporting and Control, 25 Pension Cost, 26 Transformation Strategic Alignment) as we have successfully enacted plans for IR and Pension, improved Financial Controls through the FCF project, plus benefitted from processes introduced for Business Transformation.

7. Overall our risk profile appears to have decreased: the total number of Key Risks has increased to 28, however the overall level of risk has decreased as a net of four red risks (one burnt red) have moved to amber following completion of KFAs.

8. "**Risks of the Moment**" are reported to the Board regularly in the CEO's Report. But 8 Key Risks that have been noted by Risk Owners as most current ("proximity"), e.g. potential to impact us over the next quarter, and are highlighted on the GRP by an asterisk. These include threats to our negotiations with the Government (1), with Royal Mail (11) and with BOI (12), our internal IT resilience (4) and protection of our data (14), completion of Transformation due to payroll legislation effecting our contractors (7) and the increasing complexity for the next phase (5), and keeping our people on track whilst the current reorganisation is completed (9). These are receiving particular attention from Risk Owners.

9. Other longer term, potential risks (e.g. material legal, regulatory and other external risks) are included in the **Horizon Scanning report** in section 9 and monitored by risk owners and the Legal, Risk & Governance team. Any impact is included in the evaluation of risks in the Group Risk Profile, in particular risk 13) FS Regulatory Supervision (net evaluation of 3 – 4) and 22) Regulatory Compliance Breach (net evaluation of 4 – 2).

10. **Risk incidents** following the introduction of weekly incident reporting across the business, the level of incident reporting has continued to increase. The Central Risk Team reports "significant" incidents to the GE and the business units, RCC and ARC. This informs the current assessment of risks at all levels. Fifty significant incidents were reported to the risk team since the last ARC, many of which relate to individual incidents, such as system outages (Credence) and branch crimes (robberies, frauds). The following three incidents would appear to be the most significant and are therefore reported specifically.

    a) Back office Systems

    We have experienced instability since the start of December in the back office systems, Credence and POLSAP. In particular:

POL00247018

- Credence was repeatedly unavailable on December mornings because it was unable to process high, seasonal volumes in its overnight batch run. This was compounded by a hardware failure event which caused batch job disruptions.
- An issue in the summary sales reporting led to a day's double counting in sales management information.
- An error occurred in January, also believed to be Credence related, where duplicate notifications of Lottery transactions were sent through Horizon.
- In addition in January, the Supply Chain team identified possible mis-matches between the foreign currency branch cash balances on Horizon and the balances reported on POLSAP.

b) *Access to HR SAP*

In December, the Financial Reporting Controls work identified that we had 94 individual users with "payroll manager" access to live payroll processing. The correct level is considered to be 7.

c) *Cash forecasting*

There were two cash forecasting errors made over the Christmas period which created potential operational issues for POL, requiring urgent action:

- An error was identified in the branch cash demand forecast which was understated by a day's trading. This required emergency cash remittances to be sent out to the most vulnerable branches via Royal Mail Special Delivery;
- on Friday 30th December £12.5 million of POMS' cash was used by POL to cover unexpected cash shortfalls in the network. These funds were transferred to POL mid-afternoon on Friday 30th December and were repaid by midday the next business day (Tuesday 3rd January). The transfer of the funds was not managed in accordance with the appropriate governance process.

11. Management has responded to each of these incidents. Further details and action plans are included in appendix 2.

12. There are 5 **risk exceptions** being drafted, covering areas where our risk appetite is being/ or is likely to be exceeded including Project Finch, Use of Robotics, Paystation (INGENICO), First Contact Resolution and Back Office Transformation Programme – Penetration Testing. These will be reported to the ARC once drafted and considered and the return to appetite will be tracked by the Central Risk Team.

13. **Risk and Control Environment.** In December 2016, Legal, Risk and Governance met with the Chair of ARC to discuss the measures by which we can enhance the Audit, Risk and Compliance Committee (ARC) into 2017. One of the proposals from the Chair was for development of a tool which would facilitate discussion of the risk & control environment. This tool has been discussed at the RCC and a pilot will be run in Supply Chain, and a cross functional assessment will be included of the risks owned by the Director Legal, Risk & Governance with the results being reported to the RCC and ARC in May.

POL00247018

14. Our previous **Risk Appetite Summary** (Jan 2015) has been reviewed with GE Risk Owners:

- Our previous Risk Appetite Summary has been benchmarked against other organisation's examples (including POMS, FRES) and reshaped it to reflect our new strategy, operating model and key risks.
- The mid-point risk appetite score, "neutral/ balanced", has been removed and replaced with a lowest score of "intolerable", so keeping the four point scoring model requested by ARC.
- The individual appetite statements are positioned to act as a set of "guiding principles" for Management to use when making decisions, as reference points for how much risk we should/ could take, in relationship to the potential return, and what level of mitigation is needed. Potential measures have been included as suggestions of how these discussions could be illuminated.
- A RCC working session has been arranged to test these statements using a series of scenarios, including real life decisions already taken or to be taken, to validate the statements and determine how to use them.

POL00247018

POST OFFICE

Confidential - for discussion only

Appendix 1, tab 1

GROUP RISK PROFILE - Jan 2017

Version: Updated 16th January 2017

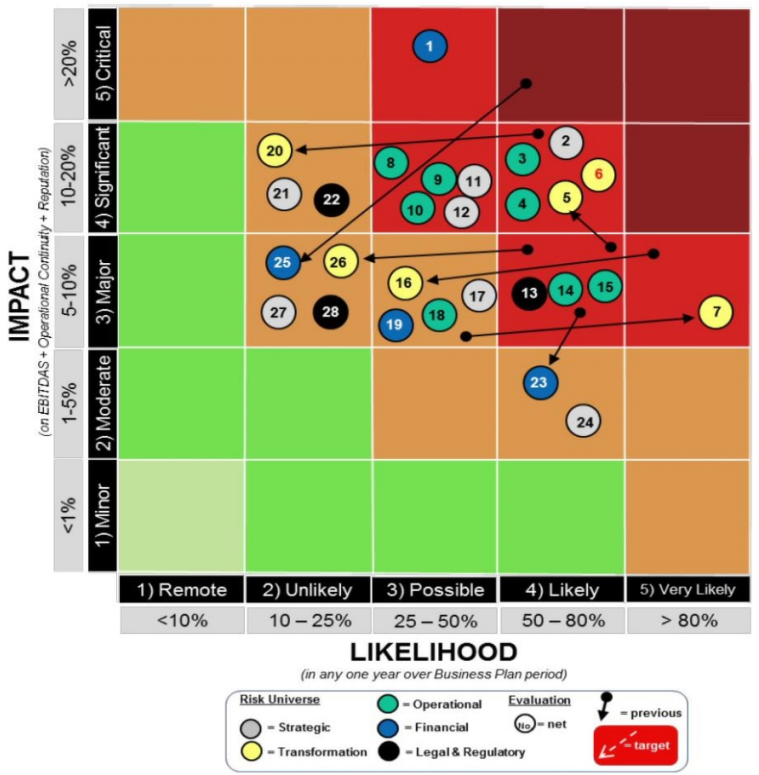
See overleaf (tab 2) for Key Further Actions, (tab 3) for Harm Table

Strategic Objectives	Targets
Our core business strategy – our path to profitability - is: • To be the Number One letters and parcels retailer • To grow financial services • To be a trusted distributor for our own products and those of others And, in so doing • To protect and deepen our social purpose by providing access to these essential services for all communities in the UK.	**Achieve EBITDAS breakeven by 2017/18**

KEY RISKS

Ref	RoM	Risk Cat	Title	Owner	Previous (Mar '16)	Change This Qu	Net (L)	Target (L)
RED RISKS - *for actioning to bring the net evaluation to the target*								
! noted by Risk Owners as most current ("proximity"), e.g. potential to impact over the next quarter, and requiring particular attention from Risk Owners								
1	!	Fin	Government Funding and Headroom	Al C	5 - 3		5 - 3	2 - 1
2		Strat	Market Developments/ Competition (Retail: Mails & Govt Services)	Kevin G	4 - 4		4 - 4	2 - 3
3		Oper	Third Party Relationship Management	Jane McL	4 - 4		4 - 4	2 - 2
4	!	Oper	IT Availability/ Ability to Trade	Rob H	4 - 4		4 - 4	4 - 2
5	!	Trans	Change Portfolio Delivery - Complexity	Al C	3 - 4	↑	4 - 4	3 - 4
6	New	Trans	IT Delivery Capability	Rob H	-	New	4 - 4	3 - 2
7	!	Trans	Transformation Resourcing - Payroll Legislation	Al C	3 - 3	↑	3 - 5	3 - 4
8		Oper	Network Proposition	Kevin G	4 - 3		4 - 3	4 - 2
9	!	Oper	People Capability	Martin K	4 - 3		4 - 3	2 - 3
10		Oper	Customer Experience	Kevin G, Nick K	4 - 3		4 - 3	3 - 2
11	!	Strat	Royal Mail Alignment	Kevin G	4 - 3		4 - 3	4 - 2
12	!	Strat	Market Developments/ Competition (Financial Services & Telecoms)	Nick K	4 - 3		4 - 3	3 - 2
13		Leg & Reg	FS Regulatory Supervision	Nick K	3 - 4		3 - 4	3 - 2
14	!	Oper	Information Security/ Data Protection Breach	Jane McL	3 - 4		3 - 4	3 - 1
15		Oper	Digital Competency	Nick K	3 - 4		3 - 4	3 - 2
AMBER RISKS - *for monitoring to alert if turning Red*								
16		Trans	Industrial Relations (Transformation)	Martin K	3 - 5	↓	3 - 3	3 - 3
17		Strat	Investments Decisions	Al C	3 - 3	-	3 - 3	2 - 2
18		Oper	FS Sales Capability	Kevin G	3 - 3	-	3 - 3	2 - 2
19		Fin	Commercial Sustainability	Al C	3 - 3	-	3 - 3	1 - 2
20		Trans	Transformation Benefit Realisation	Al C	4 - 4	↓	4 - 2	4 - 1
21		Strat	Corporate Reputation	Paula V (Mark D)	4 - 2	-	4 - 2	4 - 1
22		Leg & Reg	Regulatory Compliance Breach	Jane McL	4 - 2	-	4 - 2	2 - 2
23		Fin	Financial Reporting and Controls	Al C	3 - 4	↓	2 - 4	2 - 2
24		Strat	Government Alignment	Paula V (Martin E)	2 - 4	-	2 - 4	1 - 2
25		Fin	Pension Cost	Martin K	5 - 4	↓	3 - 2	3 - 2
26		Trans	Transformation Strategic Alignment	Al C	3 - 4	↓	3 - 2	3 - 1
27		Strat	NFSP Alignment	Kevin G	3 - 2	-	3 - 2	3 - 1
28		Leg & Reg	Health & Safety	Martin K	3 - 2	-	3 - 2	3 - 1

NET RISK PROFILE (including change from previous/ Sept '16)



Note:
- Objectives and Targets are from Business Plan 15/16 - 17/18. Used as illustrative example until updated for Business Plan 16/17 - 18/19.
- A risk's "net" evaluation is after consideration of the effect of current controls; its "target" evaluation is the estimate of where the risk will be in 12 months after the effect of planned Key Further Actions (see overleaf for details of Key Further Actions).
- For ARC/ governance purposes, Red Risks are for actioning and have Key Further Actions designed to bring the net evaluation to the target; Amber Risks are for monitoring, to alert if the risk is turning Red. Risk owners may well have Key Further Actions for amber risk, but they are not reported to the ARC.
- Further details of current controls and further actions are held by risk owners in their business area Risk Registers.

POL00247018

POST OFFICE

Confidential - for discussion only

Appendix 1, tab 2

SUMMARY OF KEY FURTHER ACTIONS (RED RISKS ONLY) - Updated Jan 2017

Red text is new for Jan 2017

Version: Updated 16th January 2017 (Key Risks noted by Risk Owners as most current ("proximity"), e.g. potential to impact over the next quarter, and requiring particular attention from Risk Owners)

Details of Risks and Evaluations

Risk Owner	Ref	RoM	Title	Description	New Jan 2017 KFAs	Action Owner	Action Target Date
Martin Kirke	9	!	People Capability	There is no clear prioritisation of capabilities required to deliver the business strategy, particularly during current reorganisation	• Implementation of new Org Design • Implement Strategic hiring • Post embedding new organisational structure, define and agree people capability gaps in People strategy	HR Directors HR Directors Martin Kirke	Jan-Sep 17 On-going On-going
Kevin Gilliland	2		Market Developments/ Competition (Retail: Mails & Govt Services)	Unable to respond quickly enough to new entrants with different strategies/ business models, current competitors with new products/ technologies, who take market share and/ or profitability	• Develop a response to the market and competitor activity for Mails • Develop new product proposals (e.g. POCA+)	Mark Siviter Tom Wechster	Mar-17 Mar-17
	8		Network Proposition	Unable to retain and or/find sufficient new retail partners because of the complexity and controls of the current proposition and value to the retailer, which leads to a decline in network numbers below 11,500	• Develop win/win proposition for agents to improve bottom line • Communicate true value of proposition to existing/ potential agents to drive demand	Tom Moran Tom Moran	Mar-17 Mar-17
	11	!	Royal Mail Alignment	Misalignment of objectives and unsuccessful renegotiation of MDA or renegotiation on disadvantageous terms	• Continue joint strategy project with RMG	Gordon Rose/ Mark Siviter	Mar-17
Nick Kennett & Kevin Gilliland	10		Customer Experience	Our customer experience, propositions and channel strategy fail to deliver what customers want	• Consider improvements to product/ customer journeys and customer complaints process once reorganisation has been completed • Review Brand experience	Nick Kennett/ Kevin Gilliland Nick Kennett/ Kevin Gilliland	Mar-17 Mar-17
Nick Kennett	12	!	Market Developments/ Competition (Financial Services & Telecoms)	Unable to respond quickly enough to new entrants with different strategies/ business models, current competitors with new products/ technologies, who take market share and/ or profitability - includes BoI is not aligned (strategically or financially) to assist POL's growth plans	• Negotiations underway with BoI (ongoing through 2017) • Plans for 100 Day Roadmap currently being assessed by GE • Submit business case for fibre broadband	Jonathan Hill Jonathan Hill Nick Kennett	Mar-17 Jan-17 Mar-17
	13		FS Regulatory Supervision	FS products are designed and distributed in a non compliant way, T&C oversight is inadequate, regulatory failure as a result of inadequate risk management, guidance or support .	• Following agreement of new approach (Network/ Legal) to resolve network regulatory conflicts of interest issues, complete Network Conduct risk remediations (inc EUM) • Following implementation of improved processes for vetting with BoI, operationalise new Vetting policy	Owen Woodley/ Jonathan Hill Martin Kirke/ Joe Connor	Jun-17 Feb-17
	15		Digital Competency	Lack of digital competency to spot and implement quickly enough (e.g. new products, customer journey, back office)	• Update to GE on plans for Digital Strategy	Nick Kennett	Mar-17
Rob Houghton	4	!	IT Availability/ Ability to Trade	Failure of infrastructure or application environments, either due to internal issues, supplier/ partner failure or cyber attack, leads to lack of IT availability and/ or inability to trade	• Perform gap analysis on Tier 1 application to identify and remediate BC/DR plans • Completion of BC/DR plans • Testing of BC/DR • Perform gap analysis on Tier 2 and 3 applications • Reshape BOTT project and progress per revised schedule	Sharon Gilkes Sharon Gilkes Sharon Gilkes Sharon Gilkes Ben Cooke	May-17 Aug-17 Dec-17 Jul-17 Sept-17
	6 New		IT Delivery Capability	Unable to deliver in line with our Transformation cost, benefit and delivery plans due to lack of strength in POL technical leadership capability, lack of continuity of key people in key roles, and/ or IT Change Programmes designed and configured around high risk single event implementations. Resulting in change either not being delivered at all or taking longer, costing more, delivering less with eroded benefits	• Review the next phases of change delivery to identify improvements and efficiencies • IT increase inhouse capabilitities including recruitment of new CTOs • IT review system infrastructure to identify what can be simplified and decoupled • IT work with vendors to agree new ways of working to break changes down into smaller manageable activities and to be more agile	Al Cameron/ Rob Houghton Rob Houghton Rob Houghton Rob Houghton	Mar 17 Mar 17 Ongoing Underway
Al Cameron	1	!	Government Funding and Headroom	Funding beyond 2017/18 is insufficient to support the investment and transformation programme and we breach our headroom requirements	• Following presentation of 5YP & Funding request, planned meeting for PV & TP with Minister • KPMG to complete Due Diligence on 5YP for Minister • Governnment funding in BEIS budget submission • Develop plan for State Aid Application • Develop plan for managing credit/ going concern if subsidy not forthcoming/ adequate • Tighten cash management	Martin Edwards Martin Edwards Al Cameron/ Paula Vennells/ Martin Edwards Martin Edwards Amanda Redford Amanda Redford	Dec-16 Jan-17 Feb-17 Mar-17 Mar-17 Jun-17
	5	!	Change Portfolio Delivery - Complexity	The next phase of Transformation will have increased dependencies and interconnectivities leading to more complexity to manage, which if not managed well could significantly impact our execution plan	• Develop a single Business and IT Master Plan to schedule and smooth Change Delivery to minimise programme interlocks and dependencies • Create a single view of all Change to avoid creating unnecessary complexity across the Change portfolio • Ensure clear lines and demarcation of accountability between Change Programmes and Enterprise Portfolio Management activities • Produce new integrated plan and identify scheduling and hotspot constraints	Al Cameron/ Rob Houghton Al Cameron/ Rob Houghton Al Cameron/ Rob Houghton Al Cameron/ Rob Houghton	Apr -17 Apr-17 Apr-17 Apr-17

POL00247018

	7	**Transformation Resourcing - Payroll Legislation**	HMRC are making legislative changes which are effective from April 17, which could cause significant impact to Transformation's current resource model and threaten our ability to deliver Transformation Phase 2. Impacts include increase in costs, reduction in number and quality of contractor resource pool	• Obtain appropriate legal/ tax advice to ensure compliant and run contractor scenarios through the HMRC guidance and confirm tax liability for templated and specialised roles • Work with Business Leads to identifty critical contractors and develop action plan/ contingency approach for each • Establish POLs requirement for the level of assurance POL need to complete where POL obtain resource through a third party supplier i.e. IT via ATOS/Accenture • Reforecast change demand planning to identify required resource and skill requirements • Engage with new preferred resource agency supplier • Develop comms plan for GE/ Exec and also contractors • HR confirm framework for mix of contractor to perm and consider potential colleagues at risk who could temporarily cover change roles	Alison Thompson/ Steve Rogers Alison Thompson/ Steve Rogers Nisha Marwaha Alison Thompson/ Steve Rogers Alison Thompson/ Steve Rogers Alison Thompson/ Steve Rogers Joe Connor/ Martin Drake	Mar-17 Mar-17 Mar-17 Mar-17 Mar-17 Mar-17 Mar-17
Jane MacLeod	3	**Third Party Relationship Management**	Fail to select, contract, measure, monitor and exit key in-source or out-source relationships/ contracts successfully and/ or unintentional breach of contractual terms by PO	• Upload contracts (top 20) into Bravo and CM training • Annual attestation of compliance with policy/ guidelines • Recruit Procurement Operations Manager to manage administrative aspects of 3rd Party Supplier Relationship Management • Draft guidelines for Relationship Management (with BOI, RMG, etc) and share with key stakeholders • Commence implementation of formal Supplier Relationship Management at PO	Heads of Legal Heads of Legal/ Compliance Barbara Brannon Barbara Brannon Barbara Brannon	Dec-16 Mar-17 Apr-17 Mar-17 Apr-17
	14	**Information Security/ Data Protection Breach**	Fail to adequately deploy and effectively manage information assurance and cyber security policies, standards and controls within the business and our partners/ suppliers, results in a breach of company data (colleague/ customer)	• Establish a Security Operations Centre (SOC) - requirements by Jan-17 • Deploy Security Incident Event Management (SIEM) • Deploy Data Loss Prevention tool	Mick Mitchell Mick Mitchell Mick Mitchell	Mar-18 Mar-18 Jun-17

POL00247018

POST OFFICE

Appendix 1, tab 3

HARM TABLE - MEAUREMENT CRITERIA

Version: 18th Feb 2016, post RCC & ARC

Use EBITDAS target of £100m

Risk Scoring	Impact on*				Likelihood of*	
	Label	Financial** (EDITDAS)	Operational Continuity (Operations, IT, Colleagues)	Reputational (Stakeholder, Customer, Colleagues, Third Party, Media, Regulator)	Label	Probability
5	Critical	>20% of financial target or significant impact on all objectives	National service disruption/ significant location/s or business function/s for >3 days	- withdrawal of stakeholder/ customers/ colleagues/ 3rd party support, or - extensive national media coverage, or - formal regulatory intervention	Very Likely	>80%
4	Significant	>10-20% of financial target or significant impact on all objectives	National service disruption/ significant location/s or business function/s for <3 days	- significant challenge from stakeholder/ customers/ colleagues/ 3rd party support, or - some national media coverage, or - formal regulatory investigation	Likely	>50-80%
3	Major	>5-10% of financial target or significant impact on all objectives	Regional service disruption/ major location/s or major business function/s for <3 days	- major questioning from stakeholder/ customers/ colleagues/ 3rd party support, or - extensive local media coverage, or - informal regulatory enquiry	Possible	>25-50%
2	Moderate	>1-5% of financial target or significant impact on all objectives	Local service disruption at several locations or business functions for >3 days	- moderate concern from stakeholder/ customers/ colleagues/ 3rd party support, or - some local media coverage, or - informal regulatory conversations	Unlikely	>10-25%
1	Minor	0-1% of financial target or significant impact on all objectives	Local service disruption at several locations or business functions for <3 days	- neglible interest from stakeholder/ customers/ colleagues/ 3rd party support, or - no media coverage, or - no regulatory interest	Remote	0-10%

*Note: * any one year over Business Plan time horizon*
*** generally use financial measure first, then enhance if an additional operational or reputational impact applies too*

Our risk evaluation can be on a basis of:	
GROSS risk	= the risk evaluation ***before*** taking into account the effectiveness of controls currently in place. Sometimes referred to as "inherent" risk.
NET risk	= the risk evaluation ***after*** taking into account the effectiveness of controls currently in place. Sometimes referred to as "residual" risk.
TARGET risk	= the risk evaluation ***if*** further actions were taken to manage the risk to an acceptable level (i.e. ultimately to meet the desired risk appetite).

POL00247018

Appendix 2: detail of recent risk incidents

a) Back office Systems

We have experienced instability since the start of December in the back office systems, Credence and POLSAP. As the ARC is aware, these old, fragile systems are the subject of the Back Office Transition and Transformation programmes. Credence was repeatedly unavailable on December mornings because it was unable to process high, seasonal volumes in its overnight batch run. This was compounded by a hardware failure event which caused batch job disruptions. The IT and supplier teams are actively reducing the impact of these issues, while working on rectifying them as part of Back Office Transition, with final delivery in Q1 2017-18.

In addition, we have seen an issue in the summary sales reporting, which led to a day's double counting in sales management information. This was manually corrected in December. Subsequently the summary tables are being re-built from first principles to ensure the integrity of the data.

An error occurred in January, also believed to be Credence related, where duplicate notifications of Lottery transactions were sent through Horizon. This was immediately identified by postmasters and is being managed as a transaction correction process. The Camelot Transaction Acknowledgement (TA) issue was resolved on 14th January. The issue was caused by an incorrect 'flag' setting within Credence. Whilst investigations continue to understand the root cause of this issue, we have put in place extra checks and monitoring to ensure there are no further re-occurrences.

In January, the Supply Chain team identified possible mis-matches between the foreign currency branch cash balances on Horizon and the balances reported on POLSAP. Reconciling cash between Horizon and POLSAP is an ongoing Financial Reporting Controls activity which has been completed for Sterling and is underway on foreign currency. The value of the unexplained differences has been reduced to £1.6m focused on two currencies, US$ and Euros and it may be that no genuine difference exists. If it does, we will clearly rectify and report it. No operational impact on our business has been identified, although we do see Postmaster complaints about process complexity and transparency.

It is not believed that any of these incidents has an impact on our financial statements. However, we must provide ourselves with positive assurance that this is the case. Our new Financial Controller, Amanda Radford, is putting together a programme of work to provide this assurance by end February. We are suggesting that we undertake this jointly with EY.

b) Access to HR SAP

In December, the Financial Reporting Controls work identified that we had 94 individual users with "payroll manager" access to live payroll processing. The correct level is considered to be 7. We have engaged Steria, the system

POL00247018

administrator, to remove these access rights and to give us the ability to assure ourselves that there has been no incorrect processing or interventions. We will confirm that with EY as part of the external audit.

c) Cash forecasting

There were two cash forecasting errors made over the Christmas period which created potential operational issues for POL, requiring urgent action.

a) On 23rd December the Bristol Inventory team started to receive calls from branches with insufficient cash to sustain trading through Christmas. The 23rd was the 2nd day of industrial action within Supply Chain. An error was identified in the demand forecast, which was understated by a day's trading. As soon as the error had been discovered a contingency working group was stood up and emergency cash remittances were sent out to the most vulnerable branches via Royal Mail Special Delivery. Over the Christmas period further cash was produced and delivered as required. No branches cashed out. The additional cost was £28k of which £19k was for using the premium RMSD service. All forecasts have been reviewed.

b) On 30th December, the Treasury team identified that lower than forecast ATM remittances from Bank of Ireland had triggered a gap in immediately available funding. While POL was operating well within its working capital facility, it had requested too small a short-term funding top-up from government and less flexibility than normal was available because of the seasonal pressures and a general tightening of forecast prudence. The problem resolved itself on the next working day (Tuesday 3rd January). Following a conversation with the CE, FS & Telecoms, and to avoid either postponing payments to suppliers or going into unauthorised overdraft, it was proposed that POL would use cash held by POMS and postpone a payment to the FRES joint venture. Formal agreement was reached with FRES. The repayment of £12.5m POMS cash and the delayed payment of £15m to FRES were made on 3rd January as agreed. Although this was not understood at the time, the transfer from POMS was not made in line with POMS's delegated authorities (it should have had Board approval) but is not considered to have been a regulatory or reportable error. The Chairman and Board of POMS have been informed and the learnings are being collated by POL's General Counsel.

A good deal of activity is underway across the management and forecasting of cash in POL, with the arrival in January of a new, permanent Treasurer and Financial Controller. We had already identified and were working on significant opportunities to improve the management of cash and its efficient use across POL. The intention is to bring the results of this work to the Board in April. The current work plan, bringing these things together is as follows:

POL00247018

Action	Accountability	Timetable
1. Undertake an end to end review of cash forecasting across three perspectives (a) branch by branch (b) POL's use of its facilities (c) the NCS overview. Agree an improvement plan with owners and a timetable, seeking opportunities to automate where possible. This will include review and sign off arrangements.	Mark Dixon	28 February
2. Identify all significant models and spreadsheets in the forecasting process. Implement the controls over models and spreadsheets identified in the Financial Reporting Controls Framework.	Danielle Goddard	31 March
3. Implement transitional checks on the forecasts (a) to ensure senior review of plans and assumptions and (b) for Treasury and Supply Chain to review and sign off each other's plans and assumptions at least until the full control environment is operating	Mark Dixon/Russell Hancock	Immediately
4. Identify improvements to the accuracy and accessibility of branch cash declarations to ensure availability of real time, accurate branch cash holdings. This will include accessibility via Credence. Create an owned, dated action plan.	Mark Ellis	28 February (underway)
5. Undertake a formal lessons learnt review, with agreed actions and decisions, for seasonal cover, workforce/resourcing contingency and operational contingency. Sign off with CFO and Head of BCP.	Russell Hancock	10 February
6. Review sources, access and controls over contingency funding – what is the optimal level, how do we manage, what emergency sources are available, how should they accessed and controlled?	Mark Dixon	31 January
7. Review and create appropriate actions for key person risks, generally and at peak periods.	Russell Hancock	31 January
8. Engage with actions from General Counsel's review of the lessons learnt from the use of POMs cash. Consider the need of POMs for cash and ensure it is minimised to those needs.	Amanda Radford/Al Cameron	As per JM's schedule (underway)

POL00247018

Implement additional POMs training for POL staff as required.		
9. As part of Back Office Transformation, replace the systems journey on cash processing to create a simple, online, end to end process designed for the agreed outcomes	Al Cameron/Amanda Radford/Ben Cooke/Russell Hancock	TBD (underway)
10. Implement an end to review of opportunities to improve headroom	Mark Dixon	31 March
11. Implement an independent review of the amended processes and approaches and lessons learnt	Internal Audit	Q1 2017-18

POL00247018

8) Business Continuity update

Author: Tim Armit Sponsor: Jane MacLeod Meeting date: 30 January 2017

Executive Summary

Context

Embedded business continuity policies and strong incident management processes are sensible risk management tools and are embedded in SYSC 8 requirements. While Post Office has a strong history of responding well to crisis and has the right people in place to manage incidents, nevertheless there are further improvements that could be made to how this is done.

A new BCP manager Tim Armit, commenced with Post Office in November. Given the range of issues faced across Post Office, he will focus on a more pragmatic, operational approach for plans and strategies across all areas.

Questions this paper addresses

- What is the current business continuity status?
- What are the next steps and priorities?

Conclusion

1. Due to the previous BCP Manager having extended health issues during the latter part of 2016, progress against the implementation of the BCP framework in accordance with the policy has been delayed. A full-time BCP manager was appointed in November and following an initial assessment period during which there were a number of incidents affecting the business (including Industrial Action, Credence outages, hack of the routers used by POL Homephone & Broadband customers, Chesterfield power outages and ongoing supplier continuity review and support), he has been able to form a view of the current state of Post Office's framework, and what activities and issues need to be prioritised.
2. The first priority will be reviews of the Crisis Communication (Business Protection Team) process and IT Disaster Recovery capability and testing, as well as the implementation and testing of the Chesterfield work area recovery solution provided by Sungard solution.

Input Sought

The Committee is requested to note the summary set out below.

POL00247018

The Report

What is the current business continuity status?

3. The role of BCP Manager was previously filled by a contractor. With effect from November we have appointed a new Business Continuity Manager Tim Armit who has military and IT experience as well as 26 years in business continuity, working for Whitehall, The Bank of England, QBE Insurance, John Lewis, Nestle and Cambridge University among others.

4. POL has strong detailed documented management systems in place to support its approach to business continuity in line with ISO Standards. The BCM will now focus on making this operational to meet business needs by the end of 2017, including developing a program of regular and appropriate tests.

What are the next steps and priorities?

Review of the Crisis Communication (Business Protection Team) process.

5. The existing BPT process is cumbersome, not including all the correct people and not targeting the right tiers of people relevant to incidents. Invocation has not been consistently applied. The BCM will review, update and test who is involved, the tiering and the invocation method with a new system (based on the police gold, silver and bronze) in place before the end of March 2017.

Review of the IT Disaster Recovery capability and testing.

6. The BCM will work with IT to reconfirm to the business what level of IT DR is in place, which systems are covered, recovery capabilities including timeframes to determine what further business planning is required around known and emergency IT downtime. This will roll out across 2017 as IT DR tests are completed.

Identification of the impacts of incidents to the business.

7. There are currently no agreed or well understood measures of impact for each business area should they be unable to operate. Without understanding the impact it is impossible to measure the level of investment required to build resilience in the operation. The BCM will co-ordinate all areas to define their impact over time to enable this before the end of March 2017.

Restructure of the continuity plans across each business area.

8. Current continuity plans are often over 30 pages long and structured as documents not as aide memoires to use during a crisis. The BCM will simplify and restructure the documentation to be more effective and usable rolling out from Chesterfield (to be completed by end of March 2017) across the key Post Office operational sites by the end of 2017.

Implementation and testing of the Chesterfield work area recovery (WAR) Sungard solution.

9. POL has had a recovery contract with Sungard for 3 years, but ownership has been unclear and it has not been possible to test it effectively. IT links, Call Centre recovery capability and desktop recovery are all required to make the site fully functional. The BCM and IT teams will initiate a project to make the site operational to enable it to be tested. Initial testing will take place in late January

POL00247018

2017 with a review after this of what else may be required. A full test relocation of the Chesterfield function will take place before the end of May 2017.

Ongoing supplier continuity review and support.

10. Key suppliers have contractual requirements for POL to demonstrate that competent levels of business continuity is in place at all time. The BCM will continue to work with all business areas to support them with this.

Ongoing support of live incidents including Credence, TalkTalk hack, Chesterfield power.

11. There are ongoing and continual significant incidents across many areas of operation. The BCM will continue to be involved in all of these at a support and operational level.

POL00247018

Horizon Scanning Report

Author: Jane MacLeod

Meeting date: 30 January 2017

Executive Summary

Context

As part of its remit, the Audit & Risk Committee should consider legal, regulatory and other external developments on behalf of Post Office in order to ensure that impacts on Post Office (including its customers, staff, suppliers and stakeholders) are understood and being appropriately managed. This report highlights current developments of relevance to Post Office and the work that is being done to monitor these.

Questions this paper addresses

1. What are the material legal, regulatory and other external risks the Post Office executive and Board should currently be aware of?
2. What work is being undertaken to assess, monitor and mitigate these risks?
3. Who is accountable for this work and how will it be reported through Post Office governance structures?

Conclusion

1. There are a number of material developments which either will or could impact Post Office and details of these are set out in this summary.
2. In each case, work is being undertaken to monitor and assess the risks arising from these developments. The Legal, Risk & Governance team is working with the different stakeholders to progress this assessment.
3. Governance structures and reporting lines will be developed to ensure there is appropriate representation from across Post Office in formulating responses to, and mitigation plans for, these developments.

Input Sought

The Audit & Risk Committee is asked to note these developments.

POL00247018

The Report

Corporate Governance Reform Green Paper

1. The Government's decision to launch a consultation on corporate governance is a sign of its continued commitment to review the way UK businesses are run. It is also a clear statement that the Government wants to increase public trust in businesses, particularly in the wake of recent high profile cases such as BHS and Sports Direct.

2. The Green Paper identifies some current issues and suggests some options for reform. There is no preferred option at this stage but the aim is to open a dialogue on the proposals. The Financial Reporting Council, the Investment Association and the Institute of Directors have all welcomed the publication of the Green Paper.

3. **Executive pay** in quoted companies is a key area of concern according to the Green Paper. Views are sought on the following areas:

- shareholder voting and other rights. Quoted companies are already required to subject their pay policy to a binding vote every three years and their annual pay awards to an annual advisory vote. The Green Paper considers options for increasing shareholder influence in this area
- shareholder engagement on pay
- the role of the remuneration committee
- transparency in executive pay
- long-term pay incentives

4. Options being considered include:

- making all or some elements of the executive pay package subject to a binding vote and introducing stronger consequences for a company losing its annual advisory vote on the remuneration report
- ways of encouraging shareholder engagement on pay such as mandatory disclosures of fund managers' voting records at AGMs and the extent to which they have made use of proxy voting
- imposing a consultation obligation on remuneration committees when preparing the pay policy
- the much discussed pay ratio reporting which would compare CEO pay to pay in the wider company workforce
- simplifying long-term incentive plans

5. **Strengthening the voices of employees, customers and other stakeholders** is another area of particular focus. Section 172 of the Companies Act 2006 already requires companies to consider the interests of other stakeholders (such as employees, suppliers and customers) in their decision making process. Views are now being sought on how to strengthen the voice of employees, customers and other stakeholders in the boardroom. Other stakeholders could include suppliers, pension fund beneficiaries and the wider society.

POL00247018

6. However, there is no suggestion that employees or other stakeholders would be directly appointed to company boards or that a dual board structure should be created echoing the comments of Theresa May at a recent CBI conference. This appears to be a clear watering down of the Government's original proposal to have employee and customer representatives on boards.

7. The consultation also proposes options such as stakeholder advisory panels and designating non-executive directors with responsibility for ensuring other stakeholder voices are heard at board level. Alternatively, a disclosure obligation could be imposed to clarify how stakeholder interests have been taken into account in board decision-making. The Green Paper considers whether the stakeholder engagement options should be subject to an employee size threshold or some other threshold.

8. Views are also being sought on whether large private companies – where they are of similar size and economic significance to public companies - should adhere to **the UK Corporate Governance Code**, a set of principles of good corporate governance aimed at companies listed on the London Stock Exchange. Alternatively, a new tailored code could be developed by bodies such as the Financial Reporting Council or the Institute of Directors. Businesses can express their views on the size threshold that should apply and whether it should be a legal requirement or a voluntary approach.

9. Corporate governance continues to be a rapidly evolving area and the publication of the Green Paper is the latest in a series of announcements. The consultation is open until **17 February 2017** and, given Post Office's good practice in this area, not least though the Post Office Advisory Council which acts as a useful vehicle for engaging a broad set of stakeholders in the work of the Post Office, the Corporate Affairs team intends to work with colleagues across the business to develop a contribution.

Criminal Finances Bill

10. The Government has introduced the Criminal Finances Bill into Parliament further to strengthen is ability to tackle money laundering, corruption and counter terrorist financing. As well as changes to the regime for recovery of the proceeds of crime, the Bill introduces a new corporate criminal offence of failing to prevent tax evasion. The Bill may be passed into law as early as Spring.

POL00247018

11. The Bill contains three main areas of reform:

- The creation of new corporate offences of failure to prevent facilitation of tax evasion. In summary, the proposed new offence will be committed where there is:
    - criminal tax evasion by a taxpayer (either a legal or natural person) under the existing criminal law;
    - criminal facilitation of that offence by a person acting on behalf of a "relevant body", and
    - the organisation in question had no available reasonable prevention procedures in place to prevent the conduct.

- Recovery of the proceeds of crime and enforcement powers, including the regime around dealing with the proceeds of crime, money laundering, civil recovery and enforcement. Law enforcement agencies will be given new powers to request information in relation to a money laundering investigation, extending the availability of existing disclosure orders used in confiscation investigations and fraud investigations. Another new power will enable the seizure of funds in bank accounts and items of value, where these are reasonably suspected to be the proceeds of crime. Changes to the Proceeds of Crime Act 2002 (POCA) will permit the sharing of information between entities in the regulated sector where they have notified the National Crime Agency (NCA) that they suspect activity is related to money laundering, a so-called "super SAR". New Unexplained Wealth Orders (UWO) will be available to require a person suspected of involvement in or association with serious criminality to explain the origin of assets that appear to be disproportionate to their known income. This power would extend to foreign politicians or officials or those associated to them (Politically Exposed Persons), reflecting the concern that those involved in corruption overseas launder the proceeds of their crimes in the UK, and the difficulties faced by law enforcement agencies obtaining sufficient evidence when all relevant information may be outside of the jurisdiction.

- The extension of money laundering and asset recovery powers to investigations in relation to terrorist property and terrorist financing under the Terrorism Act 2000 and the Anti-Terrorism, Crime and Security Act 2001, including the powers to enhance the SARs regime, information sharing, seizure and forfeiture powers and disclosure orders.

12. These new measures require close monitoring by the Financial Crime Team in Legal, Risk and Governance as the Bill makes its way through Parliament, but signal no let-up in the need for Post Office to remain extremely vigilant in ensuring that its business processes and operations continue to guard against the use of the network by criminal networks.

POL00247018

E-Privacy Regulation

13. Alongside the work Post Office is undertaking to ensure its compliance with the EU General Data Protection Regulation (GDPR) by May 2018, a leaked copy of draft legislation to replace the 2002 ePrivacy Directive emerged shortly before Christmas. This will have further impacts on our telecoms, marketing and insights activity. The data protection team in Legal, Risk & Governance are actively engaged in monitoring and managing this additional piece of legislation.

14. The draft indicates a potentially significant impact on any organisation, whether based in the EU or elsewhere, that uses metadata, tracking software or other tools to monitor online behavior. As under the GDPR, sanctions for non-compliance may reach 4% of global annual revenues.

15. Specifically, the draft Regulation envisages the following changes:

- **Regulation not Directive:** By avoiding the need for transposition into national law, the Regulation will be directly applicable and leave less room for divergent national laws.

- **Territorial scope:** The Regulation would apply to electronic communications data processed in connection with the provision of electronic communications services in the EU, regardless whether the processing takes place in the EU, and to the protection of information related to the terminal equipment of end-users in the EU.

- **Tracking tools:** The Regulation confirms that the current cookies rules apply universally to all end-users, irrespective as to whether they are individuals or corporate subscribers. The new rules critically apply a more stringent approach to consent - requiring "opt-in" consent to be secured (as defined by the GDPR) before deploying any third party or non-essential cookie. To further protect end users from unwanted tracking, device firmware and browser software must be configured to restrict these cookies by default (i.e. unless the end user subsequently accepts a cookie or changes settings). The rules extend beyond cookies and pixel tags to cover any form of tracking tool, including tools that "interfere" with the terminal equipment without storing any code on the user device (such as by using the terminal equipment's processing capabilities).

- **Communications secrecy:** Metadata from all types of providers will need to be deleted except as permissible under the current exceptions (e.g. billing, quality control or cybersecurity) or if prior consent is provided by the end-user.

- **Spam:** The Regulation confirms that anti-spam rules will apply universally to all subscribers (including both individual and corporate email addresses). Direct e-marketing will not be permitted unless the end-user has consented, or unless to existing customers for similar products (with an opt-out option required). The Regulation would permit Member States by law to conduct voice-to-voice marketing on an opt-out basis.

POL00247018

- **Breach notification:** The procedure for ISPs and telecoms providers to report breach notifications – which was introduced in the 2009 ePrivacy amendments – is to be aligned with the breach notice requirements in the GDPR.

- **Enforcement:** As with the GDPR, a violation of the e-Privacy Regulation could be fined up to 4% of the total worldwide annual revenues; data protection authorities would be given powers to enforce certain provisions of the Regulation.

16. The draft text of the proposal is expected to be finalised in **January 2017**, after which it will be reviewed by the European Council (comprised of EU Member State representatives) and the European Parliament; this process could take several months. Once finally adopted, the draft text currently provides for a 6 month transition period.