POL00401627

Post Office Risk and Compliance Committee Agenda

Date	
10 July 2018	

Start Time	Finish Time
13.00 hours	16.00 hours

Location
1.19 Wakefield, Finsbury Dials

Present	In Attendance		Apologies
Jane MacLeod (Chair) Paula Vennells Al Cameron Meredith Sharples Tom Moran	Jenny Ellwood Johann Appel Jonathan Hill Paul Beaumont David Meldrum Barbara Brannon Sally Smith	Sarah Koniarski (Secretary) Lisa Toye (Secretary)	

Agenda Item	Action Needed	For ARC	Purpose	Lead	Time
1. Welcome and Conflicts of Interest			Members to declare any conflicts of interest.	Chair	13.00 – 13.05 (5 minutes)
2. Minutes and Action Lists	Approval		To approve the minutes of the meeting held on 2nd May 2018 and update on actions.	Chair	13.05 – 13.10 (5 minutes)
3. Risk Update		✓			13.10 – 13.40 (30 minutes)
3.1 Risk Report	Questions & Noting		To review the risk report.	Jenny Ellwood	
4. Internal Audit		✓			13.40 – 14.00 (20 minutes)
4.1 Audit Report	Questions & Noting		To note the Internal Audit Report for onward submission to the ARC.	Johann Appel	

CONFIDENTIAL

Post Office Risk and Compliance Committee Agenda (cont.)

Agenda Item		Action Needed	For ARC	Purpose	Lead	Time
5.	**Compliance**		✓			14.00 – 14.45
	5.1 Compliance Report	Noting		To note the Compliance paper	Jonathan Hill	(45 minutes)
	5.1.1 IDD Update	Questions & Noting		Verbal IDD Update	Jonathan Hill	
	5.1.2 PSD2 Update	Questions & Update		Verbal PSD2 Update	Jonathan Hill	
	5.2 Vulnerable Customers Risk Assessment	Input and Discussion			Paul Beaumont	
6.	**Contracts Governance Update**	Input and Discussion		Update on non compliant contracts	Barbara Brannon	14.45 – 14.55 (10 minutes)
7.	**Updates for Noting**					14.55 – 15.10 (15 minutes)
	7.1 PCI-DSS Compliance Status Update	Noting	✓	To note the update on PCI-DSS Compliance Status.	David Meldrum	
8.	**Policies for Approval**		✓	To agree for onward submission to the ARC.		15.10 – 15.30
	8.1 Gifts and Hospitality Policy	Approval			Sally Smith	(20 minutes)
	8.2 Anti-Bribery and Corruption Policy				Sally Smith	
	8.3 Whistleblowing Policy				Sally Smith	
9.	**Future Meetings**	Input and Discussion		Discussion on scheduling and content of future meetings.	Jane MacLeod	15.30 – 15.50 (20 minutes)
10.	**Any Other Business**				Chair	15.50 – 16.00 (10 minutes)
	CLOSE					16.00

Post Office Limited
Risk and Compliance Committee Meeting

MINUTES OF A MEETING OF THE RISK AND COMPLIANCE COMMITTEE (THE "COMMITTEE") OF POST OFFICE LIMITED (THE "COMPANY") HELD ON 2 MAY 2018 AT 20 FINSBURY SREET, LONDON EC2Y 9AQ AT 10.00AM

Present:	Jane MacLeod	Chairman	
	Paula Vennells (PV)	Group Chief Executive	
	Al Cameron (AC)	Chief Financial and Operations Officer	
	Rob Houghton (RH)	Group Chief Information Officer	
	Joe Arakji (JA)	(on behalf of Martin Kirke)	
	Tom Moran (TM)	(on behalf of Debbie Smith)	
	Chrysanthy Pispinis (CP)	(on behalf of Owen Woodley)	
In Attendance:	Jenny Ellwood (JE)	Risk Director	
	Johann Appel (JA)	Head of Internal Audit	
	Jonathan Hill (JH)	Compliance Director	
	Deana Herley (DH)	Senior Assurance Manager	*1 – 3*
	David Gemmell (DG)	GDPR Programme Manager	*6.1–6.2*
	Jules Harris (JH)	Head of Information Protection and Assurance	*6.1-6.2*
	Sarah Koniarski	Secretary	
Apologies:	Debbie Smith (DS)	Chief Executive, Retail	
	Martin Kirke (MK)	Group HR Director	
	Owen Woodley (OW)	Chief Executive, Financial Services and Telecoms	

ACTION

1. WELCOME, INTRODUCTION AND CONFLICTS OF INTEREST

1.1 The Chairman welcomed those present to the meeting and confirmed there was a quorum. There were no conflicts of interest declared.

2. ACTION LIST

2.1 The Action List Status Report was noted as accurate. There were no actions due which had not been addressed in advance of the meeting or through the meeting papers.

3. RISK UPDATE

Top Risks, Executive Declaration and Risk Management Section for ARA

3.1 JE introduced a paper which updated the top risks and executive declaration results. The Committee was asked to review these, together with the draft principal risk statements in the Annual Report and Accounts (ARA) 2017/18. The top risks had been based on feedback from all GE members providing a consolidated view across the Post Office business. The Committee was asked to consider whether any additional disclosures to the principal risks were required for inclusion in the ARA.

3.2 JE provided the following summary:

(a) Referring to the profile of top 12 risks, JE explained that three new top risks had been identified since the half year review: PCI-DSS accreditation; key-man dependency in Banking Services and FS&T; and sustainability of the business model. None of the new risks had created new principal risks, although they did relate to the existing principals.

(b) Three increased risks related to digital competency, safety compliance and business recovery / disaster recovery plan and testing limitations.

(c) Three reduced risks related to technology and business interruption, retail proposition and the ability to achieve "effective" GDPR compliance.

(d) Four risks were no longer deemed top risks but would continue to be managed by the respective teams with responsibility for those areas.

(e) The executive declaration returns had been reviewed by the Group Executive for materiality and consistency against Internal Audit and wider business assurance reviews. The resulting 12 items of materiality were summarised in Appendix 2 to the report. One item of material significance proposed for disclosure in the accounts as a contingent liability was the Post Office Group Litigation. To date, the amount of damages sought was unquantified and a formal state of claim was awaited.

(f) Appendix 3 to the report included an overview of the proposed principal risks mapped against the relevant top risks and executive declarations.

3.3 The following points arose in the ensuing discussion:

(a) FS&T Market Developments / Competition: The Committee reflected on the ongoing negotiations with the Bank of Ireland (BoI). Although BoI was increasingly receptive to agreeing a deal, it remained too early to be confident of securing an agreement which would further Post Office's strategic objectives. It also remained difficult to plot a reliable timeline for delivery. Performance of Financial Services and Telecoms products was a core element of the Annual Operating Plan. The Committee recognised the challenging market conditions which included competitive new entrants together with fast paced advancements in technologies. The Committee agreed that FS&T market developments and competition was a top risk and recommended its ranking be increased accordingly.

(b) Retail Proposition: The Committee was concerned that presenting a decreased risk was not reflective of the present situation. The likelihood of the risk materialising had decreased but its potential impact had increased. The Committee understood that the scoring (which demonstrated likelihood versus impact) would be provided to the Audit, Risk and Compliance Committee ("ARC") but would not be published in the ARA. The Committee asked JE and TM to review its position, with a view to increasing its ranking, before submission to the ARC. TM provided an update on the risk of disengagement by Co-Op Group (TCG) and regional Co-op Societies which would result in a reduction of Post Office estates unless performance improved. A joint working group had made good progress towards increasing their engagement by demonstrating how financial performance could be improved. JE and TM would update the item within the executive declarations to reflect recent developments. It was felt that references to the risk of 'disengagement' would be better described as 'risk of significant negotiations' in the context of recent talks.

(c) Few Key Individuals: It was agreed that any reference to 'key man' dependency throughout be amended to 'key person' dependency and capability. The Committee discussed remedial action including succession planning and providing additional capability. The importance of investing in collective 'bench strength' (increasing individuals' skill sets and subject matter knowledge) was recognised. JA referred to quarterly succession planning meetings and undertook to feedback the Committee's comments on the need to effect cultural change and enable a broader number of reports to gain exposure which would strengthen their skills in preparation for greater ownership of their respective areas.

(d) Safety Compliance: The Committee discussed whether the ranking of risk was reflective of its status. The Committee concurred that the ARA should reflect the importance of safety compliance and demonstrate that it was taken seriously across the organisation, as well as showing the improvements which had been achieved. Accordingly, it was agreed that safety compliance would be maintained as a top risk but renumbered to a lower ranking. JE would work with AC to restructure the comments to demonstrate the encouraging audit findings, the implicit difficulties in managing the risk (due to the wide scope of activities within the business) and the work of Safety Champions to improve performance in Supply Chain.

(e) Sustainability of the Business Model: The Committee agreed to remove the reference to the Group Litigation which was already captured as a separate risk.

(f) FS Regulation: The Committee agreed that AML (Anti-Money Laundering) regulation be highlighted in addition to IDD (Insurance Distribution Directive) requirements.

(g) Agents Pay IT: The Agent Remuneration Transformation (ART) project had completed successfully and was running as business as usual. The Committee understood that agents were being paid through CFS having been migrated from POLSAP and the project-specific risk had closed. There continued to be a risk of not delivering agents' pay which would be monitored as part of business as usual. JE would update the comments to reflect this. The Committee agreed it was appropriate to change the status of this risk to 'closed'.

(h) Royal Mail Industrial Action: The Committee agreed this continued to be a risk and noted that a Post Office internal contingency plan was in place.

(i) Digital Competency: The Committee agreed that this risk should be reallocated as a responsibility shared by the GE with significant support from Human Resources. Following review of the linked proposed principal risks (Appendix 3) it was agreed that digital disruption should be highlighted under the External Environment heading.

(j) DR / BCP Plans: The Committee understood that the comments would be updated in April following tests in Chesterfield and Bolton. AC confirmed that Belfast could not be tested until migration from POLSAP to SAP CFS was completed and Swindon remained a vulnerability. JE would work with AC to update the comments before submission to the ARC. RH added that the lack of support for branches open outside of 'ordinary' business hours (on Sundays for example) was a significant risk to service delivery. Service level agreements did not provide 24 hours' cover meaning there were periods when branches were open without support. RH suggested a gap analysis exercise be carried out to review contractual provisions, identify operational vulnerabilities and determine whether these were within risk appetite or whether mitigating actions were required. RH would discuss the approach with DH.

(k) Emerging risks: The risk of a growing culture of bullying/harassment and the risk of brand erosion (taking account of brand protection and brand relevance) were identified as topics to be explored in future risk work, although no changes to the 2017/18 ARA were recommended. Brand erosion would be explored as part of the rollout of the Placemat in Communications. Further work would also be carried out in relation to Change risk, to identify and mitigate the top risks within the Change programme, including the new 2018/19 plan which would be reviewed for approval by the Investment Committee. Any resulting changes to the risk profile of the Group would be reported to the ARC.

(l) In light of its deliberations, the Committee asked the Chairman to review the descriptions within the principal risks to ensure their emphasis and tone reflected discussion and aligned to the North Star strategy. The Committee suggested that individual reference to Industrial Action under Operational and Financial Risks be removed. A Legal and Regulatory risk pertaining to Group Litigation would be provided as an optional inclusion for ARC to review. Narrative under the External Environment would be expanded and the Committee recommended the Chairman seek the ARC's view on whether an amendment to specify "changes to the interpretation of a workers' status" would be appropriate. The Committee was mindful of references to the Taylor Review (Good work: The Taylor review of modern working practices) included in the Chief Executive's foreword and the materiality of the risk. It was understood that the CWU (the Communications Workers Union) had continued to challenge the status of agents, proposing that agents should be regarded as workers and a claim had been lodged through ACAS (the Advisory, Conciliation and Arbitration Service). If it progressed there would be some interdependencies with the Group Litigation. The Committee was keen to avoid an implied presumption that the risk to the business model was particular to the status of agents as workers. Project Starling had been established to consider the Taylor Review and wider issues. Its outputs would inform strategic decisions about the evolving business model.

3.5 Subject to the amendments provided, the Committee agreed the proposed changes to the top risks, noted the executive declaration outcomes and confirmed the approach to ARA disclosure as set out in the report for onward submission to the Audit, Risk and Compliance Committee.

DH left the meeting.

4. KEY OPERATIONAL RISKS

Financial Services Conduct Risk Update

4.1 The Financial Services Conduct Risk Update was noted.

4.1.2 AC highlighted the continued risk around out of date branch literature and the importance of demonstrating progress to the ARC. AC queried whether a digital solution was available. JH would review and include an update in future reports.

Change Risk Update

4.2 The Change Risk Update was noted.

4.2.1 JE confirmed that the May ARC report would provide a brief update on the Back Office Transformation and a full update in July. JE would remove Appendix 1, (internal targets for Change management) prior to submission to the ARC.

4.2.2 The Committee was mindful that the ARC had previously requested further detail as to the lessons learned from Change activity over the past three years, and a forward view as to where the principal risks would arise. JH and JE were working with the Chairman to reshape reporting to the ARC from July onwards.

Financial Crime Risk Update

4.3 The Financial Crime Risk Update was noted.

IT Risk and IT Controls Framework Updates

4.4 The IT Risk and IT Controls Framework Updates were noted.

5. INTERNAL AUDIT

Audit Report

5.1 The Internal Audit Report was noted.

5.1.2 The Committee reviewed performance against reporting service level agreements and asked **JA to consider how the reporting and clearance process for IA reports could be streamlined to speed up reporting to the ARC.** At present, there was a challenge in reaching sign off as the reports were initially reviewed by line managers and subsequently, by the relevant GE member(s) prior to Committee. This created a dependency on the availability of key individuals. The Committee suggested that particular thought be given to how report contributors were trained / supported and where GE review was necessary, whether it could be concurrent with line manager review. Turning to recurring control themes and root causes analysis, the Committee suggested an explanation of the remedial action being deployed would be helpful, such as reference to the ongoing control improvement projects. **JA**

5.1.3 It was agreed that the following reports would be provided to the May ARC meeting:

- Back Office Transition (Lessons Learnt)
- SuccessFactors Payroll (Lessons Learnt)
- GDPR Programme
- Project Mercury (Previously Solar HNGT Lite)
- Network Transformation
- Financial Controls Framework.

5.1.4 JA would work with the GE to update the summary of overdue actions prior to the ARC.

6. UPDATES FOR NOTING

DG and JH joined the meeting.

GDPR Programme Update

6.1 DG provided an update on the Post Office programme to achieve compliance with the General Data Protection Regulations ('GDPR') which would come into effect in May 2018. DG reported significant progress since the last programme update resulting in an increased certainty of achieving 'effective' compliance by 25 May 2018 and 'substantive' compliance within the 2018/19 financial year. Contract remediation, however, was a high risk area which remained a potential barrier to achieving effective compliance by the May deadline. The Committee understood that all existing contracts needed to be updated to reflect GDPR requirements. The volume of work represented a significant challenge which had been compounded by a relatively late start to the work.

6.1.2 The contracts work stream had been accelerated with activities for Post Office Management Services Limited and the IT Tower Vendors being prioritised as material contracts. DG drew the Committee's attention to the UK Information Commissioner's statement which provided an indication of the expectation regarding compliance at the May deadline. The Post Office's commitment to compliance, and its role in increasing consumers' trust regarding management of their personal data, would be key considerations should any regulatory scrutiny arise. The Committee noted that a delivery plan would be produced to detail the route to substantive compliance within the current financial year.

6.1.3 A GDPR compliance audit by PwC had highlighted that Post Office was ahead of the marketplace and specifically the financial services benchmark. Responding to questions, DG explained that the complexity of contract remediation had been underestimated resulting in an under-sized resource and a delay to the initiation of the work stream. The Committee observed that a greater understanding of the challenges, following early engagement with the business, would have assisted planning and informed a strategic approach from the outset of the project. The Committee acknowledged that organisational constraints had also had an adverse impact. There had been difficulties in accessing information, gaps in corporate knowledge and a shortage of subject matter skills and competencies. With reference to the programmes management across the organisation, the Committee reflected that an understanding of the scope of each business case and the key dependencies it shared with the overarching programmes would be beneficial.

6.1.4 The Committee noted the report and the material risks to effective compliance identified within, which would continue to be monitored by the GDPR programme steering committee.

6.1.5 The Chairman asked DG to thank the GDPR Programme team for their work to date.

PCI-DSS Compliance Status Update

6.2 JH presented an update on compliance with the Payment Card Industry – Data Security Standards (PCI-DSS). The Committee understood that the Post Office was required to obtain an annual external audit verified attestation on compliance. The existing attestation had expired on 28 December 2017 meaning there was a risk that Global Payments (Post Office's card acquirer) could levy penalties against the Company. Remediation plans had been shared with Global Payments and it was expected that accreditation would be received by 31 July 2018. To date, Global Payments had not taken action.

6.2.1 The Chairman expressed concern that the emerging situation was complex and would require greater understanding to ensure a solution which would not only expedite certification but would also future proof the route to compliance. The Committee was concerned that failure to achieve the verified attestation on compliance by 31 July 2018 could adversely impact the Banking Framework. Accordingly the Chairman would raise the issue at the next GE meeting and a report would be provided to the ARC.

6.2.2 JH advised that Fujitsu was on course to fix all of its items by mid-April but ComputaCenter (CC) (which was now also included within the scope of accreditation) had struggled to complete required actions within an acceptable timeframe. RH suggested that the report to ARC would need to demonstrate a plan of action, referencing the challenges identified together with a list of the avenues explored / exhausted to date. RH would escalate the matter to senior management within CC if needed.

6.2.3 The Committee noted the update on compliance with PCI-DSS.

JH and DG left the meeting.

7. POLICIES FOR APPROVAL

IT Security Policy (Updated)

7.1 The IT Policy had been updated to incorporate all of the additional security standards.

7.1.2 Recognising the policy's links to Change programmes and projects, JE had contacted Hazel Freeman to offer her support.

7.1.3 Responding to questions, the Chairman advised that work to provide assurance against the controls supporting the policy framework would be rolled out during 2018/19. The format of policies had been amended in preparation to include reference the risk(s) they addressed, together with the mitigating control(s) and to identify who was responsible for applying the controls and how frequently they would be applied. JH would be leading an engagement programme to improve understanding across the organisation.

7.1.4 The Committee agreed the changes to the IT Security Policy and recommended the updated policy for onward submission to the ARC.

8. ANY OTHER BUSINESS

8.1 There being no other business, the Chairman closed the meeting at 12.10pm.

....

Chairman **Date**

Post Office Limited Risk and Compliance Committee
Action List

Status Report as at: 02/07/2018

Meeting Date	AP ref	ACTION	Action Owner	Due Date	STATUS	Open/ Closed
20/07/2017	**1781**	**Insurance Distribution Directive -** Provide a briefing on the potential training requirements of the IDD in order to consider the future compliance burden against capacity in the branch network.	Jonathan Hill	10/07/2018 (July RCC)	Update at March RCC: A plan for initial training on IDD has been written and shared with Post Office Insurance (POMS). A working group would agree the training plan and focus on CPD. JJ advised that he would have a clearer picture of what was needed for implementation in the coming weeks. As POMS was the principal and POL was the appointed representative. Ian Holloway and Jonathan Hill would update on progress at July RCC with a report detailing the requirements, what had been done and what would be done to comply, including timescales.	Open

POST OFFICE
RISK AND COMPLIANCE COMMITTEE

Consolidated Risk Report, including an update on Risk Exceptions

Author: Jenny Elwood Sponsor: Jane Macleod Meeting date: 10 July 2018

Executive Summary

Context

The Post Office Central Risk team has been strengthened by the transferring of the business risk teams from Change, IT, Information Security, Financial Services and Telecoms and Supplier Assurance into the Central team. This change will now enable us to support the business areas to manage risk in a more holistic way, identifying common themes and trends, including risk interdependencies and emerging risks and ultimately improve reporting to RCC and ARC.

This consolidated risk report will continue to evolve over time, as we strive for increased integration of risk MI, insights and trends. As a first step in that journey, this paper brings together previously separate reports. Its purpose is to provide the RCC with the latest version of the Placemat, which now includes results from IT, HR, Communications, Strategy and Identity Services, the current top portfolio risks, where we are with the development of the Strategic Portfolio Office and change delivery improvements, and the current status of Risk Exceptions.

Questions this paper addresses

1. What are the key risks identified from rolling out the placemat in IT, Identity Services, Communications, HR and Strategy?
2. What are the next steps in embedding the placemat approach?
3. What is the current change portfolio delivery status and key delivery challenges?
4. What are the current top portfolio risks and where are we with the development of the Strategic Portfolio Office and change delivery improvements?
5. What is the current status of Risk Exceptions?

Conclusion

1. The Placemat approach has changed the historical, top-down, way of completing risk assessments to a more objective view of top risk alignment. This has given Post Office a deeper understanding of its risk profile.

2. Through engagement in workshops with over 70 teams, the implementation has encouraged a dialogue around the operational risks by business area and has prioritised remedial activity to reduce the impact of the highest risks.

3. The final roll-out of the Placemat to the areas of IT, Identity Services, Communications, HR, and Strategy has taken place. A full update is shown in paragraphs 10- 15. For IT the rollout provided affirmation that the top risks identified through their existing risk process remained the same, for Identity Services discussions were around their early thoughts on their strategy so as the proposition progresses the risk landscape could change.

This roll out has not identified any risks which change the current Top Risk's agreed at May's ARC.

4. Our aim is to develop further our risk management maturity and the Placemat process to further embed a more mature risk culture and enhance risk oversight and reporting, improve awareness, controls and assist in identifying business priorities. Next key steps include:
   - quarterly placemat refresh to improve the completeness and quality of risk and control information;
   - identify and work through the strategic risks for Post Office;
   - equip and enable the business to manage/report their operational risks;
   - enhance the risk exceptions process; and,
   - construct a dashboard which represents the key principal risks (referred to as 'horizontals') to provide improved insight to Executives and SteerCo's and further embed risk framework governance, oversight and reporting.

5. The next scheduled full Placemat re-assessment will be brought back to ARC in September.

6. The top portfolio risks remain i) Risk of increased costs and delayed benefits through late delivery of Change and ii) EUM effectiveness. These are relatively stable and mitigation work continues. The development of the Strategic Portfolio Office and improvements in change delivery continues at pace. A full update is provided in paragraphs 17 to 24.

7. There are 9 live Risk Exceptions for noting, shown in appendix 3.

Input Sought

8. The Committee is asked to review and comment on the report.

The Report

What are the key risks identified from rolling out the placemat in IT, Identity Services, Communications, HR, and Strategy?

IT

10. During quarter 1 we introduced the placemat to IT. There are 51 risks in total, including 11 high risks and 3 top risks. The reassessment of risk has resulted in a 15% reduction in the number of high risks compared to the previous quarter. This is the result of better processes and controls, most notably due to the completion of the Horizon Datacentre refresh programme and ensuring that our key admin and cash centres have primary and secondary connections available to reduce service interruption. The 3 top risks are detailed below, with further improvements expected over the next 4 months:

- **POLSAP** - is the remaining highest risk system and will be until Sept / Oct (dependent on delivery progress), when Cash Processing (already live in Belfast) is planned to migrate all other cash centres onto a new system, and our financial and sales processes are re-modelled and deployed onto CFS (our more modern ERP):

Risk Title	Risk	Current RAG	Mitigation Plan	Due date	Target RAG
POLSAP Legacy Systems	Failure to ensure all components are fully supported by the appropriate levels of adequate technology, hardware, whilst programme activities are in progress, may lead to a loss of service within Supply Chain and Finance Teams, resulting in service unavailability, financial loss, reputational damage and Security Vulnerabilities.	20 I/L 5:4	a) POLSAP Processes migrated to core finance. b) Migrate cash processing off POLSAP to Transtrack CWC, already live in Belfast. c) POLSAP Hosting Contract Extension – period April 1st to December 31st 2018. d) FJ Network Upgrade complete, removing security risk of old switches (reducing the likelihood of security incidents) e) POLSAP spares being reviewed monthly, currently remaining within tolerance.	a) 25.09.18 b) 25.09.18 c) 31.12.18 d) Complete e) Ongoing	6 I/L 3:2

- **Fujitsu Failover Horizon Datacentre Failover Test –** The decommissioning of POLSAP from Fujitsu is scheduled to take place in September 2018. It is recommended by Post Office IT and Fujitsu that we carry out a full recovery exercise at a suitable Bank holiday weekend in Spring 2019, as this will give contingency in the event of any issues being encountered, following the earlier decommission:

Risk Title	Risk	Current RAG	Mitigation Plan	Due date	Target RAG
Horizon Datacentre Failover Test	Failure by Post Office IT to ensure that a full Disaster recovery test is carried out on a regular basis in line with contractual agreements, may lead to being unable to restore primary servers and services not being restored in a real outage. Resulting in financial losses, reputational damage, and prolonged service interruption.	20 I/L 5:4	a) Ensure that all planned tests that Fujitsu have agreed are implemented over the next 11 months. b) Branch Database failover scheduled for the 31st August 2018. c) Failover test scheduled Easter 2019.	a) 31.12.18 b) 07.09.18 c) 26.04.19 d) Ongoing	6 I/L 3:2

Risk Title	Risk	Current RAG	Mitigation Plan	Due date	Target RAG
			d) Monthly IT Service Continuity reviews in place.		

- **PCI Compliance** – Post Office are without a Report on Compliance (RoC) from external qualified security assessors (QSA) proving our compliance to the Payment Card Industry – Data Security Standard (PCI-DSS). However, we believe that our environment has no Data or IT security exposures. We are continuing to work closely with our stakeholders, ensuring they have visibility of our remediation plan. Both the Acquiring bank and Qualified Security Assessor (QSA) are comfortable we are addressing the risk of non-compliance and a Steering Group has been set up to oversee the remediation work, explore more strategic solutions and will continually re-assess this risk:

Risk Title	Risk	Current RAG	Mitigation Plan	Due date	Target RAG
PCI Compliance	The 2017 PCI Audit identified a number of Audit Actions across IT 3rd party suppliers which are "not yet compliant". Failure by Post Office to address these findings and provide a robust plan to resolve these actions within an estimated timescale of 12 – 24 months, may result in challenges during external audits, require remediation activities and attract unbudgeted remediation costs. Ultimate penalties could result from Post Office failure to not evidence a plan of works towards compliance e.g. failure to obtain the required certification and reduce our ability to develop our strategy where it requires us to be fully PCIDSS complaint.	12 I/L 4:3	a) Conclude audits and work through the current identified actions for FJ and CC All scheduled to complete end of October 2018 b) Initiate a Programme to scope PCI compliance strategy (Project Manager / Co-ordinator) and run within IT4IT with Service Operations sponsoring c) Plan for 2018 audit scope d) Set up a business engaged e) Introduce compensating controls on any non-compliances that will not be closed by 31st July and work with QSA / Acquiring bank. f) QSA states that we are not at immediate risk of penalties or sanctions and this will be continually reassessed	a) 31.10.18 b) In progress c) In progress d) 05.07.2018 e) 31.07.18 f) On-going	6 I/L 3:2

Identity Services

11. For Identity Services, the risks are reflective of the developing stage for their business. 10 risks have been identified with the top 3 amber risks being:

Risk Title	Risk	Current RAG	Mitigation Plan
Supplier Risk	The risk of inadequate and/or ineffective procedures to select and manage technology suppliers. This could result in slowing down product development and services, leading to loss of market share	9 I/L 3:3	a) Key person risk and lack of flexibility with suppliers; b) Capability of the supplier to deliver requirements; and c) Strategic and operational alignment with suppliers.
Market proposition including product and competitive -ness risk	The risk to Identity Services' ability to exact a product offering to meet the needs of the customer, and keeping pace with the market to remain competitive	8 I/L 4:2	The Identity proposition is currently being worked through, and once developed it may have an impact on the risk profile. In the meantime, the following mitigations are being progressed: a) An agile strategic business model which can respond to emerging markets and new entrants, by reducing the time to deliver new processes and technological changes; b) The attractiveness and relevance of the product and services proposition, to meet the customer and market expectations; and c) The ability to maintain a market leading competitive advantage and to support continued sponsorship of Government products and services.
Data Protection	The risk of development and launch of sub-standard products	8	a) Design of product will be in line with industry required DP and IT standards

and Information Security	with inadequate DP and IT security. This may result in regulatory action and/or adverse media coverage leading to financial and potential reputational loss	I/L 4:2	b) Appropriate pen and security testing will be undertaken

Communications

12. Communications have identified 13 risks, with the following top red risk:

Risk Title	Risk	Current RAG	Mitigation Plan
Fragmentation of relationships with UKGI impacting effective communications and working methods	There is a risk that working relationships with UKGI become more fragmented, as a new teams beds in and roles are clarified, leading to less effective delivery of our business and governance strategies. Wholesale staff changes at UKGI seem to be resulting in multiple approaches o colleagues across the business, with previous practice of a more centrally co-ordinated system of information flow coming under some strain. A potential policy sponsorship role within BEIS itself is a welcome development, but will make the need for effective coordination more pronounced.	12 I/L 4:3	We are developing a framework document with UKGI, which ought to set out the roles, responsibilities, communication, and reporting requirements more clearly. In addition, the corporate affairs team continues to work with UKGI to develop greater understanding of the two organisations' needs through, e.g., joint team workshops, the second of which is planned for later this month.

Human Resources

13. HR have identified 54 risks with the following 5 top risks:

Risk Title	Risk	Current RAG	Mitigation Plan
Industrial relations	There remains a risk of industrial action as a result of Pay, CDC Pensions, DMB strategy and/ or a conflation of these.	16 I/L 4:4	Significant work has been done to mitigate the impact including dialogues with stakeholders, national collective engagement framework and contingency planning. Previous industrial actions have resulted in minimal disruption of service to our customers and did not receive any significant media coverage.
Digital competency	There is an ever increasing reliance on, and demands of, services through the digital medium. The Post Office strategy is to continue to enhance its digital offering as part of its 'North Star' strategy. Failure to attract, retain and develop appropriate competence would adversely affect the growth strategy and business model and could result in financial and reputational loss and regulatory sanctions.	12 I/L 3:4	a) Working with CIO to identify additional channels to attract talent b) Digital workplace programme established c) Digital workplace lead and Office 365 trainer to be hired d) SuccessFactors e-learning in place e) Digital Stars network being established f) Investment in Business Innovation Centre (101 Finsbury Pavement)
Key person dependency	There is a significant amount of business knowledge and experience covered by a few key individuals. This key person dependency is a risk to our North Star strategy which will be impacted significantly if these key individuals suddenly left the business	12 I/L 4:3	a) Quarterly meetings in place with GE members and their direct reports to discuss succession plans, 'flight' risks and high potential team members b) New handover process c) Training and development needs identified for talent.
Breach of employment regulation and legislation	Breach of employment regulation and legislation is an increasing risk due to the increasing legislation, and in light of recent judgements	8 I/L 4:2	a) The Post Office has been managing this risk through policies, companywide communications, engagement strategy and periodic training.
Agency status	There is a risk that undetermined status of Agents could result in regulatory intervention which could have a significant impact on the sustainability of our business model.	10 I/L 5:2	a) Developments in case law related to this are being closely monitored

Strategy

14. The risks identified by the Strategy team relate to delivery of their responsibilities, as oppose to the strategic risks to the Post Office. The latter will be addressed through the Central Risk team work (see paragraph 16). The Strategy team has identified one key amber risk relating to dependence on key personnel. Plans are in place to use interns to capture the knowledge to ensure continuity and minimise the impact of the sudden departure of key personnel. This risk is reported through the wider HR key person dependency risk.

15. Please refer to Appendix 1 for the completed Placemat. Please note that during the period being reported upon, the focus has been on rolling-out the placemat to the five remaining business areas. The risk position for other business areas (Retail, FS&T, LRG and F&O) remains the same as was reported in March 2018.

What are the next steps in embedding the placemat approach?

16. Our aim is to improve our risk management maturity to support the delivery of North Star ambitions and strategic priorities, while keeping the business compliant, resilient and sustainable. Appendix 2 provides our assessment of where we are now and where we aspire to be. The next phase of the Placemat roll-out will further embed the risk framework to enable enhanced risk oversight and reporting, through:
    - quarterly placemat refresh to improve the completeness and quality of risk and control information. This will include risk and control descriptions, scoring rationale and consistency, principal risk consolidation and linking through the connected events to support the view, such as Audit findings and incidents;
    - identifying, assessing and managing strategic risks to Post Office achieving its North Star ambitions and delivering on its strategic priorities;
    - Develop executive reporting and oversight perspective on the 'top risks'. Reviewing more closely those risks which, if not monitored and managed, could create harm to the Post Office and its strategic objectives;
    - simplifying the risk exceptions process and exploring ways to digitise it providing greater effectiveness and efficiency in raising and subsequently approving, monitoring and reporting of exceptions; and
    - constructing a dashboard for the key principal risks currently being piloted for Financial Crime, Safety and Information Security. The dashboard will provide a view of how Post Office is performing against the relevant principal risks pulling together performance and risks MI (including results of any recent assurance/audit work) enabling us to track risk performance and where we are against risk appetite.

What is the current change portfolio delivery status and key delivery challenges?

10. In June 2018 the HNGT Lite business case was reporting red from a delivery perspective due to unallocated Cloud Enablement costs causing the

financial position to be in exception. Since then the costs have been correctly allocated and the financial position updated. The programme delivered a functioning pilot to the June Board and is on track to deliver the first Live Retailer POS-integrated pilot sites in August. The programme is reporting Amber whilst a PCI issue is resolved in the underlying infrastructure. This has the potential to push the date out but the current position is that the impact should be limited to one week's slippage.

11. The capability delivered by HNGT Lite programme is being taken forward into a new business case later in July.

12. Back Office Transformation has amended its go live date to September 2018 and is reporting Amber. Challenges remain as there is little contingency. At this point the programme is around 45% through its second integration test cycle with a 78% pass rate. This is slightly behind plan. High volume validation of settlement and billing calculations against historical data are in progress and are matching expected results for the POLSAP Migration Project, but issues have been found with process & technical system performance which are being worked through. A 3rd party has been engaged to review test coverage and provide a report on suitability. The challenges of completing the build and testing of the cash processing project remain. Mitigations have been implemented. The residual risk is that cash processing plans are tight.

13. Key achievements secured since the last ARC include:
    - Customer Hub: The Post Office Travel App went live in June 2018 with some low risk activities outstanding. As full update is provided in the separate Compliance report.
    - General Data Protection Regulations (GDPR): GDPR came into force in May 2018. Through adopting a risk-based approach, we have essentially secured 'effective compliance' with the requirements of the new legislation, although we did not reach the desired level of contract remediation. Work continues to improve the position on material contracts by end of July. A full update on reaching 'substantive compliance' is provided in the Compliance report.

What are the current top portfolio risks and where are we with the development of the Strategic Portfolio Office and change delivery improvements?

14. The current portfolio top risks remain i) Risk of increased costs and delayed benefits through the late delivery of Change and ii) EUM effectiveness.

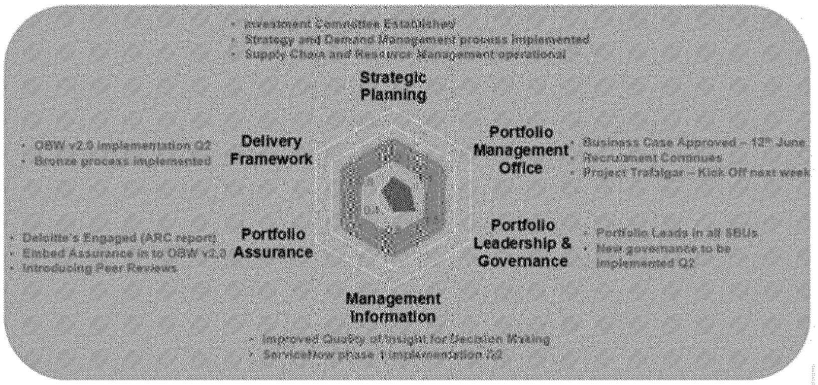
15. In terms of the overall portfolio we currently have **18** active change portfolio risks but the Change Risk & Assurance team are currently undertaking a comprehensive review to ensure they remain consistent with the change challenges currently facing the Post Office. This work will be completed by end July 2018 at which point the portfolio risks will be re-baselined. The output of this work will be provided to ARC in Sept 2018.

Late delivery of change and an update on the Strategic Portfolio Office

16. In November 2017, the GE endorsed analysis which concluded that due to systemic problems the current change capability was not mature enough to deliver the strategic outcomes of the business and recommended changes to structure, governance, culture and competency to address these issues. They approved a £500k seed investment for the Assess phase.

17. In January 2018, PA Consulting undertook a maturity assessment of the current capability against other organisations operating in the retail and financial services market. PA rated Post Office at 1,[1] out of 5, compared with an average score of 3.5 and 4 respectively. Since then a high-level design for a new change target operating model (TOM) has been developed and work is now underway to implement this so that we can address the fundamental issues and attain the necessary maturity levels required to fulfil our strategic goals.

18. A key objective of implementing this TOM will be to increase the maturity from 1 to 3 within 12 months (around June 2019), to mitigate the systemic issues identified and to establish the foundations for continuous improvement thereafter. An update on the activities to drive up the capability maturity model is shown below.



- Investment Committee Established
- Strategy and Demand Management process implemented
- Supply Chain and Resource Management operational

Strategic Planning

Portfolio Management Office

- Business Case Approved – 12th June
- Recruitment Continues
- Project Trafalgar – Kick Off next week

Portfolio Leadership & Governance

- Portfolio Leads in all SBUs
- New governance to be implemented Q2

Management Information

- Improved Quality of Insight for Decision Making
- ServiceNow phase 1 implementation Q2

Portfolio Assurance

- Deloitte's Engaged (ARC report)
- Embed Assurance in to OBW v2.0
- Introducing Peer Reviews

Delivery Framework

- OBW v2.0 implementation Q2
- Bronze process implemented

19. A more focused Investment Committee is in place and a new UKGI quarterly reporting framework and the establishment of a new Strategic Portfolio Office.

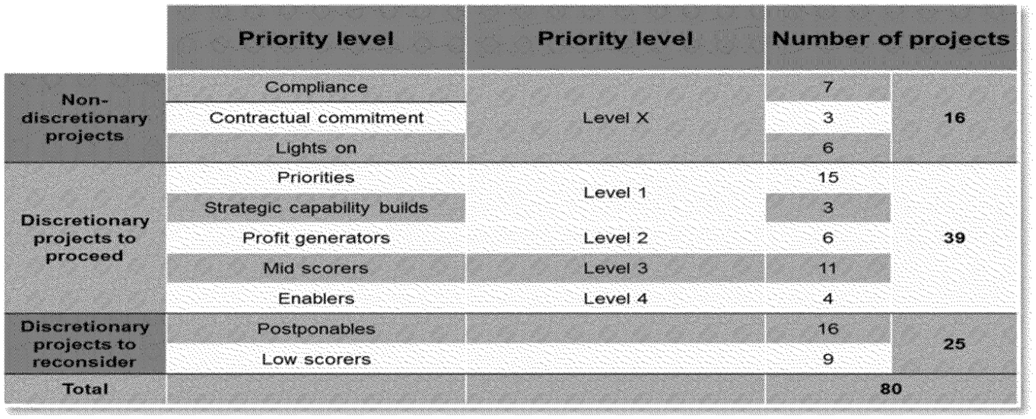
20. Following Investment Committee approval of the Business Case in June 2018 work is underway on the delivery of Phase 1. This is targeted for completion by September 2018. Key deliverables in this phase include:
    - a full Agile Business Case and an implementation roadmap;

[1] Capability Maturity Model Integration (CMMI) Level 1 (Initial) –whilst processes exist they are not always fit for purpose, nor are they consistently applied or adequately governed and consequently the organisation is often reactive in its management.
CMMI Level 4 (Quantitatively Managed) – This builds on level 3 practices and uses statistical and other quantitative techniques to understand performance variation. It identifies and understands variation, and predicts and improves the ability to achieve quality and process performance objectives.
CMMI Level 5 (Optimizing) – This builds on level 4 practices and uses statistical and other quantitative techniques to optimize performance and improvement to achieve quality and process performance objectives.
In practice it is expected that the Post Office will probably achieve 4 in some dimensions and only 2 in others thereby achieving an overall average of 3.

- detailed funding plan for Phase 2;
- development of a Post Office Scaled Agile Framework (SAFe)[2]; and,
- continued implementation of quick-wins including the recruitment of key roles into Strategic Portfolio Office.

21. Phase 1 also includes the development of a prioritised Investment Portfolio for 2018/19, the introduction of One Best Way improvements and enhancements to governance. This includes replacing the existing Change Approvals Group with Change and Portfolio Performance Review Committees to provide better focus.

22. The SPO is undertaking a prioritisation and optimisation exercise on the change portfolio. This involves an assessment of the pipeline of future programme and projects against set criteria to ensure we focus on delivering those Change initiatives which deliver the North Star and financial goals whilst generating the optimal returns on investment within an acceptable risk envelope. This has been initially assessed by the portfolio managers of the respective business units and then subject to peer review. This work being reviewed and managed at the Investment Committee but is summarised in the following table.



	Priority level	Priority level	Number of projects	
Non-discretionary projects	Compliance	Level X	7	16
	Contractual commitment		3	
	Lights on		6	
Discretionary projects to proceed	Priorities	Level 1	15	39
	Strategic capability builds		3	
	Profit generators	Level 2	6	
	Mid scorers	Level 3	11	
	Enablers	Level 4	4	
Discretionary projects to reconsider	Postponables		16	25
	Low scorers		9	
Total			80	

23. Work has also been initiated on integrating risk & assurance lessons learned into core processes and building a Competency Assessment and Development Plan for the wider change community. Deloitte have been briefed on the TOM to ensure the appropriate controls and assurance are being implemented to address the lessons learned. We await a copy of their report and recommendations.

24. Finally, we have also recently commissioned Deloitte to undertake some separate work on the emerging change assurance model to provide

[2] SAFe is the leading industry framework for implementing Scaled Agile and will be tailored to meet the specific needs of the Post Office.

additional assurance that the way forward, and progress against it, is sufficiently comprehensive and robust.

Risk Title	Risk	Current RAG	Mitigation Plan	Due date	Target RAG
Late Delivery of Change	Our change is delivered late, risking costs and benefits or has unintended consequence	**15** **I/L: 3:5**	• Phased Transition plan: phase 1 developed and actively being tracked, stories are being implemented using an agile methodology. Objective is to treble maturity in 12 months. • Project prioritisation: Ideation collection and prioritisation process developed. Initial prioritised project list shared at Investment committee on 23/4 • Investment committee: in place, ways of working will develop and be improved as Investment Committee and support forums mature. • Strategic portfolio office: ○ launched ○ recruitment completed ○ target operating model phase 1 ○ target operating model phase 2	31/7 31/7 Complete Complete 30/9 30/9 31/3/19	**6** **I/L: 2:3**

Enhanced User Management (EUM)

25. The EUM delivery plan is progressing well. As at 25 June, the Programme had rolled out the new identity solution to 3,885 branches (an increase of over 1,400 branches since the last ARC submission) and is on target to achieve over 6,000 branches by end of July. This equates to 20,000 individual users in our largest branches covering over 90% of POMS sales. We are also seeing improved training compliance for Smart ID branches at 89% for individuals. Unfortunately, it is not possible to directly compare to non-Smart ID branches as individual performance data is not gathered.

26. The collection and cleansing of agent and agent assistant data is still a key dependency for EUM. Based on current response levels, we estimate a non-conforming tail of around 1,900 branches by the end of the programme. A tail management plan is underway to address this, including issuing a single Smart ID to the branch owner and disabling all other Horizon IDs. This would following an intensive period of chasing, including branch visits to minimise the numbers of branches impacted.

27. The programme is still planning full roll-out by November 2018 and deployment of training controls to commence in October 2018 and complete by January 2019.

28. To support this transition the programme have completed the design of a structured set of measureable go/no-go criteria around switching on the training controls beginning in October 2018. A GE update is planned for August 2018 so that the risk profile of implementing training controls for the first group of branches is understood and agreed before the programme takes action.

Risk Title	Risk	Current RAG	Mitigation Plan	Due date	Target RAG
EUM	There is a risk that EUM does not perform as expected due to • being unable to collate accurate data from agents • POL staff/agents not having an individual email address	**12** **I/L: 4:3**	• Branch Standards: Uplifted team in place although recruiting continues for final 2 FTE resource. New Branch Standards Team Supervisor in place to manage the new FTEs, share	Complete	**9** **I/L: 3:3**

Risk Title	Risk	Current RAG	Mitigation Plan	Due date	Target RAG
	which can be used to communicate logins and training information **(resolved)** • Agents not being able to access SuccessFactors via the internet/browser solution **(resolved in new design)** This all leads to our inability to address the key business goal, which is for POL to prove to its client that persons transacting on its behalf are suitably qualified and vetted.	■	knowledge and manage escalations. • Horizon/LMS interface: to ensure continuity/integrity of training data is in build. Technical integration is now live, with final Horizon changes being implemented as part of Release at end of July 2018. • EUM: Escalation plan implemented by Common Services team to chase branches data capture, this includes dedicated NBSC team calling branches. EUM currently is currently on track to be live in over 6000 branches by end of July 18.	12 July 30/7	▨

What is the current status of Risk Exceptions?

29. There are 9 current approved Risk Exceptions for noting.
    - 7 new Risk Exception Requests (RER) were approved since the last report. Of these, 4 relate to the Customer Hub;
    - 1 RER relating to Robotics was closed; and
    - 3 RERs relating to SalesForce, SuccessFactors and Call Centre Recording have overdue action(s).

30. The details of the existing and new Risk Exception Notes can be found in Appendix 3.

31. As mentioned in paragraph 16 above, the Central Risk team are also simplifying the risk exceptions process and exploring ways to digitise it to enable greater effectiveness and efficiency in identifying, analysis, reviewing, approving, monitoring and reporting of risk exceptions.

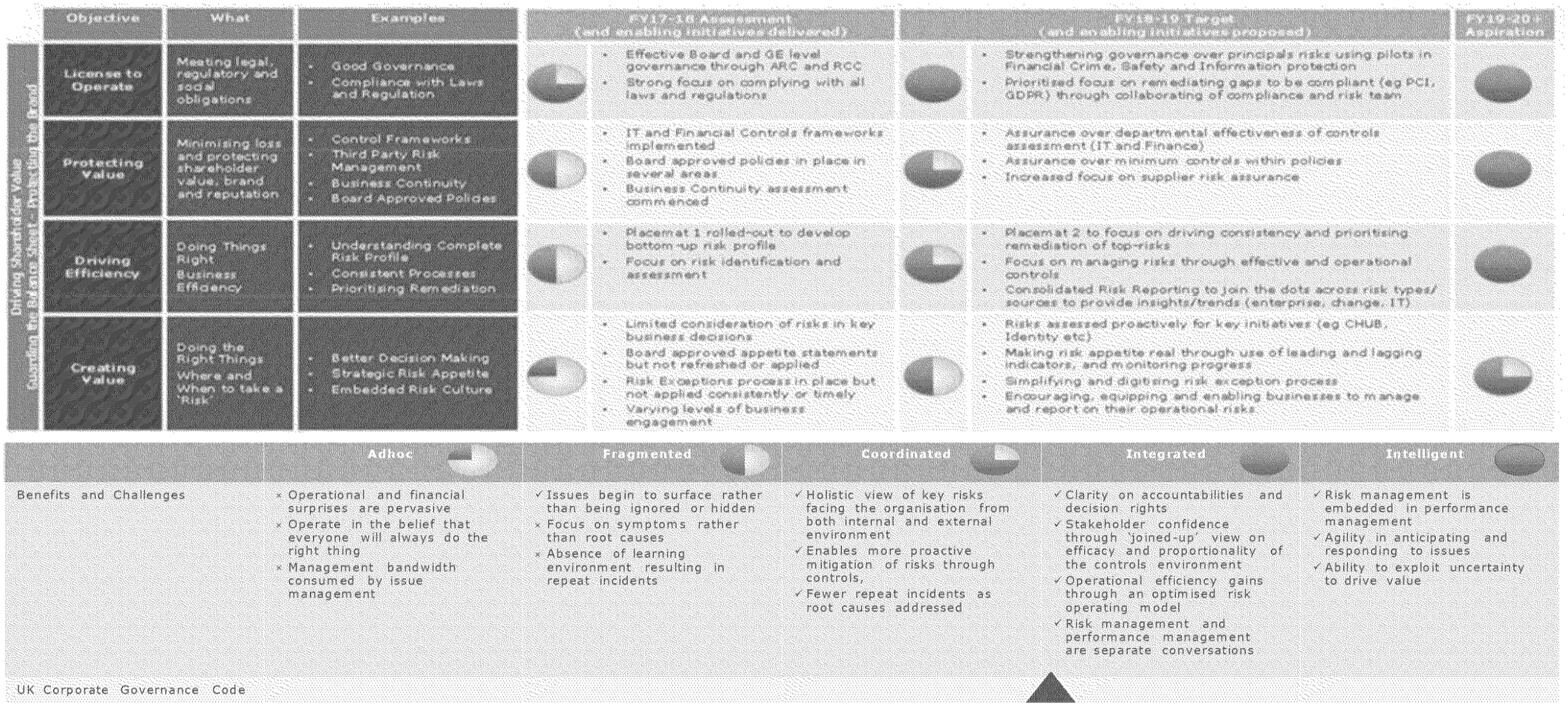
Appendix 1: Placemat

To follow

Appendix 2: Embedding Placemat – Current Maturity and Forward Plan

We have assessed the maturity of our risk management framework against observed good practices using Deloitte's maturity model. The table below outlines our assessment against the different attributes in terms of where we are today (at the end of FY17-18) and what activities supported this; our target for FY18-19 and what interventions we propose to make; and our aspiration for FY19-20 and beyond. These take into consideratioin the benefits that each stage of maturity provide to the organistion.

We believe that our plans will allow us to realise benefits from risk management in the pursuit of our North Star Ambitions and build confidence in the delivery of our strategic priorities, but also help us to align with the principles that underpin the spirit of the UK Corporate Governance Code in a proportionate manner.



Driving Shareholder Value
Guarding the Balance Sheet – Protecting the Brand

Objective	What	Examples	FY17-18 Assessment (and enabling initiatives delivered)		FY18-19 Target (and enabling initiatives proposed)		FY19-20+ Aspiration
License to Operate	Meeting legal, regulatory and social obligations	• Good Governance • Compliance with Laws and Regulation	◕	• Effective Board and GE level governance through ARC and RCC • Strong focus on complying with all laws and regulations	●	• Strengthening governance over principals risks using pilots in Financial Crime, Safety and Information protection • Prioritised focus on remediating gaps to be compliant (eg PCI, GDPR) through collaborating of compliance and risk team	●
Protecting Value	Minimising loss and protecting shareholder value, brand and reputation	• Control Frameworks • Third Party Risk Management • Business Continuity • Board Approved Policies	◑	• IT and Financial Controls frameworks implemented • Board approved policies in place in several areas • Business Continuity assessment commenced	◕	• Assurance over departmental effectiveness of controls assessment (IT and Finance) • Assurance over minimum controls within policies • Increased focus on supplier risk assurance	●
Driving Efficiency	Doing Things Right Business Efficiency	• Understanding Complete Risk Profile • Consistent Processes • Prioritising Remediation	◑	• Placemat 1 rolled-out to develop bottom-up risk profile • Focus on risk identification and assessment	◕	• Placemat 2 to focus on driving consistency and prioritising remediation of top-risks • Focus on managing risks through effective and operational controls • Consolidated Risk Reporting to join the dots across risk types/ sources to provide insights/trends (enterprise, change, IT)	●
Creating Value	Doing the Right Things Where and When to take a 'Risk'	• Better Decision Making • Strategic Risk Appetite • Embedded Risk Culture	◔	• Limited consideration of risks in key business decisions • Board approved appetite statements but not refreshed or applied • Risk Exceptions process in place but not applied consistently or timely • Varying levels of business engagement	◑	• Risks assessed proactively for key initiatives (eg CHUB, Identity etc) • Making risk appetite real through use of leading and lagging indicators, and monitoring progress • Simplifying and digitising risk exception process • Encouraging, equipping and enabling businesses to manage and report on their operational risks	◕

	Adhoc ◔	Fragmented ◑	Coordinated ◕	Integrated ●	Intelligent ●
Benefits and Challenges	× Operational and financial surprises are pervasive × Operate in the belief that everyone will always do the right thing × Management bandwidth consumed by issue management	✓ Issues begin to surface rather than being ignored or hidden × Focus on symptoms rather than root causes × Absence of learning environment resulting in repeat incidents	✓ Holistic view of key risks facing the organisation from both internal and external environment ✓ Enables more proactive mitigation of risks through controls, ✓ Fewer repeat incidents as root causes addressed	✓ Clarity on accountabilities and decision rights ✓ Stakeholder confidence through 'joined-up' view on efficacy and proportionality of the controls environment ✓ Operational efficiency gains through an optimised risk operating model ✓ Risk management and performance management are separate conversations	✓ Risk management is embedded in performance management ✓ Agility in anticipating and responding to issues ✓ Ability to exploit uncertainty to drive value
UK Corporate Governance Code			▲		

Appendix 3: Risk Exceptions

Title (Type) and Risk	Owner	Date	Actions	Due Date	Status/ Update
SalesForce – Procurement (Regulatory) Contract has been renewed / extended non-compliantly for a period of 12 months.	GE-Owen Woodley Accountable-Chrysanthy Pispinis	Raised: 21-Apr-17	POL should seek to run a full compliant procurement as soon as possible to reduce the risk of a challenge.	29-Apr-18	**Overdue.** - We intend to award a new compliant contract to Salesforce under the Software Reseller Framework, recently awarded to Specialist Computer Centres Plc ("SCC"). This is more cost-effective and flexible than previously identified via CDP and Accenture. The Salesforce contract expired on 29th April 2018. To finalise negotiations, Salesforce have since executed two 30-day extensions, the 2nd of which expires on 29th June 2018. The PO and Salesforce legal teams are currently finalising contracts
Success Factors (Regulatory) Implementation of Success Factors without addressing certain data protection and information security risks could result in breach of data protection regulation and Post Office policy requirements as line managers can download, copy, export and distribute, personal data of their team members, via non-corporate devices.	GE-Martin Kirke Accountable-Martyn Lewis	Raised: 02-Jan-18	Directive from Group HR Director for declaration to be signed by the staff in HR Service Centre	08-Jan-18	**Closed**.
			Weekly report to monitor access via IP addresses of non-corporate devices	08-Jan-2018	**Closed–** No longer required due to action 3.
			Installation of a password manager	26-Jan-18	**Closed.**
			Suitable training and information during the roll out of SuccessFactors (SF) to all line managers and new joiners.	08-Jan-18	Measures to be put in place: - **Closed.** - **On-going, to be included in the 18/19 compliance test.** Compliance training Info Sec/DP, updated module content to reflect.
			A corporate solution (combination of SSO/BYOD)	30-Jun-18	**On-going/ will not be completed on time. Exception will be renewed in July 2018.** • An effective temporary solution was introduced limiting all those with wide access to employee data to accessing only from their work machines. This covers all HRSC staff, will remain in place until SSO provides the restriction. • Wide access to employee data is controlled by SF roles • SSO is a part of the JML project which received funding approval last month, the team has now been mobilized. SSO for SF will be deployed first, plans indicate by Mid-July. • BYOD has been rolled out for all phones for email, but it does not cover SF, nor does it cover external laptops (planned to be rolled out over the next couple of months). • SSO & BYOD as described above will not adhere to the purpose outlined above. A 2nd stage to the JML project is to deploy rulesets for groups to limit access to our network. The HRSC team / other users who require wide personal access to data, will be placed into a group that limits access to SF on our network. The temporary solution will remain in place until such time. • Design discussions are occurring on whether BYOD (inTune) can be extended to control SF access when partnered with SSO/MIM. In the case this is possible the control will be extended. • A control is now in TrAction – to confirm monthly that access has not been granted to any user who is not technical limited to our network. Recommendation is either A) that we close this reporting point due to the preventative & reactive controls already in place, or B) report back again in 4-6 months on situation with a view to close at that time.
Contact Centre Call Recording data storage in EEA (Regulatory) Data storage at rest is not compliant with Post Office's Government contracts - There is a very small risk that personal data relating to Government	GE-Al Cameron Accountable-Gayle Peacock	Raised: 04-May-18	All call recordings will be encrypted at rest	15-May-18	**Overdue.** Will be implemented when the new solution will be delivered by Verizon. Implementation date awaited.
			Call recordings will be stored for no longer than needful.	15-May-18	
			No identifiable personal data for government clients to be collected	15-May-18	

services would be included in call recordings. - The recordings will be encrypted and held securely in Oslo.			Any changes to the status of data held in the EEA to be monitored	On-going	
			Obtain permission from clients linked to the FOCS contract to retain call recordings dealing primarily with transactional (non-personal) data off-shore within the EEA.	04-Nov-18	**Not yet due.**
Deferred Checking Pilot (Risk Appetite) Pilot relies on a physical mandate being held by PO branches and checked whenever a TimeSaver customer uses the service, potentially exposing PO to financial crime, fraud or financial loss.	GE-Debbie Smith Accountable-Greg Lewis	Raised: 01-Mar-18	As a preventative control clear branch communications will be sent out to the Post Office branches using TimeSaver together with the customer indemnities for their branch. As the service is rolled out further additional branch focus articles will be written. Clear instructions will also be detailed on the pouches advising branches not to hand out to customers who are not signed up to the TimeSaver service. For this pilot, the manual mandate process is the only option, but Post Office is looking at what technical solutions could be available that will enable an 'online' check of the mandate at point of sale.	31/07/2018	**Not yet due.** **Completed.** The workshop has taken place. To progress further engagement with ATOS is required to understand and cost options and progress if deemed worthwhile under a separate business case.
			As a preventative control participating Banks are only offering the TimeSaver service to established customers, not all customers (as this reduces their risk and liability under the indemnity to Post Office). The banks will assess the suitability of their customer for the service.		**Completed.** This is embedded in the service offering.
			The product team will monitor branch discrepancies and escalate any significant issues for further investigation to the Financial Crime Team	Weekly from 17/5/18	**Completed.** This is embedded in the service offering. No discrepancies have taken place in the pilot to date.
			TimeSaver is designed to allow efficient queue management, and to speed up the deposit process rather than increase the level of cash over Post Office counters. Increase in cash levels is being considered as part of the Future of Cash Business Case.	Business case being presented to Board on 16/5/18	**Completed.** No action required within pilot.
			Additionally, the pilot will be evaluated before the service is rolled out further. Feedback will be sought from branches who have customers using the service	Evaluation from July 2018	**Not yet due.** The pilot has not yet completed its 8 week duration
Customer Hub - Accessibility (Policy) The Customer Hub app does not currently conform to WCAG 2.0 or an agreed set of Cust Hub accessibility requirements yet. This could risk a customer mounting a legal challenge against the Post Office for not making the app accessible enough or meeting WCAG compliance to level AA.	GE-Owen Woodley Accountable- Hose Carbajo	Raised: 01-Jun-18	Hub will target WCAG compliance following IDD travel insurance changes being implemented for Sept 2018, as implementing in advance will incur significant rework and cost.	31-Dec-18	**Not yet due.**
Customer Hub - Encryption (Policy) The Customer Hub app and the back end system use varying encryption techniques which are incompatible.	GE-Owen Woodley Accountable-Bay	Raise: 01-Jun-	As part of the migration of CDP from UKCloud to the new infrastructure provider, a new full encryption service will be provisioned. This will provide the ability to use 'convergent encryption' and thus email and phone number fields can be encrypted and encryption will be performed in	31-Oct-18	**Not yet due.**

It's not possible to encrypt the email address /phone number data items since these are the critical fields needed for the search.			equivalent of the Hashicorp vault service. Unless the approach / architecture of storing Customer details changes, the Hub will mitigate the risk as part of the CDP transition timescales		
Customer Hub - Twilio Contract (Regulatory) The Twilio MSA will not be signed by the launch date of 11 June. Twilio services can be used in advance of MSA being agreed, but doing so means using service under Twilio's standard t&cs and will need funding by credit card on the account.	GE-Owen Woodley Accountable- Francisco Pazo Couto	Raised: 05-Jun-18	Contract to be signed by 30 June 2018	30-Jun-18	**Closed.**
Customer Hub - FRES Contract (Regulatory) PO is in process of negotiating a side letter to the Travel Money Card Arrangements agreement between POL, FRES and FISA Payments. FIS have not been involved in the negotiations to date and will be asked to consider the terms of the side letter once POL and have FRES have reached agreement. The agreement is not binding without FIS's approval, and as this is a tripartite agreement this poses a significant risk to POL in that FIS may reject or wish to renegotiate terms	GE-Owen Woodley Accountable- Francisco Pazo Couto	Raised: 30-May-18	An email will be sent to BOI UK and FRES (the JVCo) for them to confirm the ownership of the API and the process to be followed should FRES wish to leverage the technology and licence separately in the future.	31-May-18	**Closed.**
			The contract negotiations are near completion. POL is aiming to conclude negotiations with FRES by 8th June, and it is expected that FIS review will be completed by 15th June.	15-Jun-18	**Closed.**
			FRES will obtain the approval of its board of directors and shareholders to its accepting and implementing the terms of the side letter.	30-Jun-18	**In-progress.** The request to approve the Letter has been sent to BoI's shareholder representative, following which it will be countersigned by the authorised signatories of FRES and BoI. POL's shareholder representative has formally approved the Letter.
Lawyers on Demand (Regulatory) The Legal Team has no capacity to deal with Peregrine and Cust Hub. The decision was made and approved by the project owners that external legal support should be brought in to support the 2 projects. The Legal Team engaged with other external providers and legal firms. None of them was able to provide a candidate that is suitable for this role with the relevant experience. Due to the stringent deadlines, it was not viable to run a public procurement process to appoint LOD as a service provider. This risk exception was to approve the Legal Team to engage with LOD and on-board them as a supplier without going through the public procurement process.	GE-Owen Woodley Accountable- Francisco Pazo Couto	Raised: June 2018	There is no mitigation. The resource will be in place until such time that the two projects do not require legal expertise	N/A	**N/A**

Internal Audit Report

Author: Johann Appel Sponsor: Jane MacLeod Meeting date: 10 July 2018

Executive Summary

Context

The purpose of this paper is to update the Committee on the PO Internal Audit activity and key outcomes. This includes details of the work completed since the last Risk and Compliance Committee (RCC) and Audit, Risk and Compliance Committee (ARC) meetings in May and progress on delivery of the Internal Audit Plan.

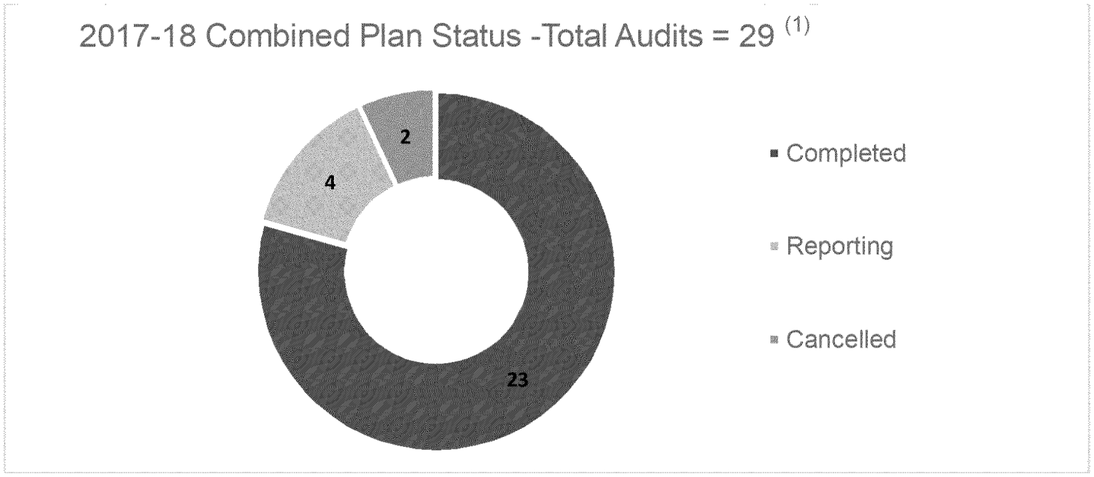
Questions this paper addresses

- Is the Internal Audit Plan on track? What progress has been made since the May RCC meeting?
- What progress is being made with completion of audit actions?
- Have any significant issues arisen that the committee should be aware of?

Conclusion

1. Progress against plan (2017-18):

Three reviews have been finalised since the May ARC meeting. The 2017-18 plan is now substantially complete with the last four reviews in the final stages of report clearance. Progress against plan is shown below:

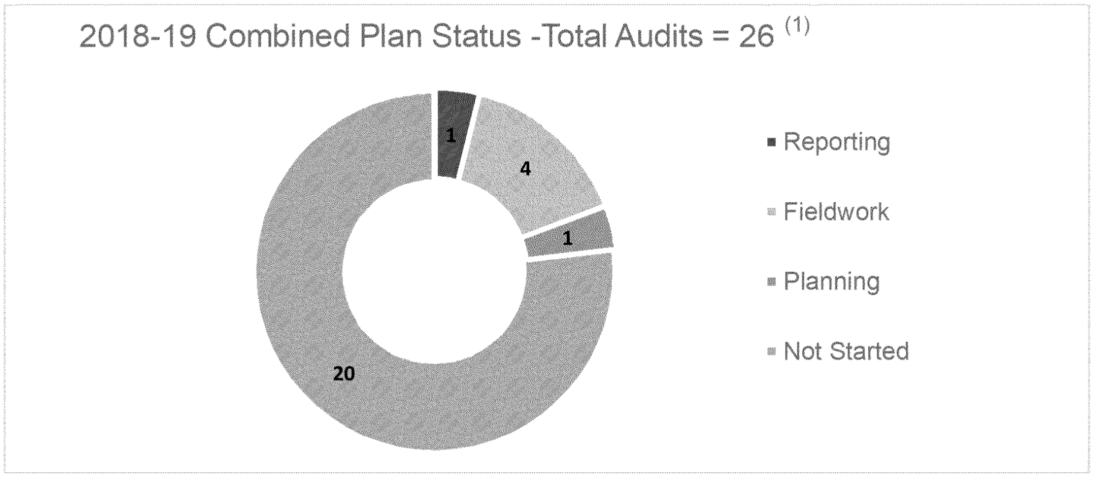


[1] ARC approved baseline plan for 2017-18 (16 internal control reviews & 13 change assurance reviews)

A full summary of the 2017-18 audit plan status is included in **Appendix 1**.

2. Progress against plan (2018-19):

Progress in Q1 has been slower than expected. This was due in part to two vacancies and the team finalising prior year audits, as well as resources being directed to the POMS audit plan and the team supporting other activities. Current delivery progress is as follows:



[1] ARC approved baseline plan for 2018-19 (16 internal control reviews & 10 change assurance reviews)

A full summary of the 2018-19 audit plan status is included in **Appendix 2**.

3. Open and Overdue Audit Actions (as at 29 June 2018):

Audit Action Status:	
Open (not yet due)	27
Overdue (<60 days)	12
Overdue (>60 days)	0
Total	39

More detailed information is provided in paragraphs 9 - 10 of the report.

4. Significant Issues:

There are no significant issues we believe the committee should be made aware of.

Input Sought

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

The Report

Changes to the Audit Plan since May RCC and ARC meetings

5. There was one addition to the audit plan:
    - Month-end Close Process – This is included in the core process rotation plan for 2019-20, but will be brought forward to the current year plan in light of the recent failure of month-end controls to identify errors in the accrued revenue for Telecoms.

Internal audit reviews completed

6. The following three reviews were finalised since the May ARC meeting:
    - EUM
    - Branch Technology
    - Business Continuity Management (BCM)

    Below are summaries of these reviews:

Audit	**Key Messages**
EUM In-flight review (Ref. 2017/18-05) Needs Improvement ***Sponsor:*** *Debbie Smith* Audit actions: P1 | 1 P2 | 3 P3 | 3 Total | **7**	The objective of this review was to assess the level of confidence in delivery of the re-designed EUM solution that was approved by the Board in January 2018. We conclude that the EUM programme has made significant progress since the previous in-flight review. Project leadership has led the re-design of the solution and gained stakeholder support for the revised business case and solution. The composition of the Steering Committee has changed to include key stakeholders from affected programmes (e.g. HR Transformation), and effective governance is in place around delivery. However, there remain some key challenges that the programme will need to address and therefore this report has been rated 'Needs Improvement'. Specifically the audit found that: • The programme needs to focus on addressing the unwillingness of branches to adopt Smart IDs, and effectively manage its dependency on the Common Services Programme in relation to the data capture process, as the quality of the data provided by the latter is key to the rollout of Smart ID. • There is a requirement to have a high level of branch and business engagement to minimise intervention for data capture and support the migration to Smart ID and training compliance completion. The programme plan needs to be reviewed to ensure dates for design milestones are achievable, and underlying assumptions of the plan need to be validated once release dates from Fujitsu are received. • Formal go / no-go decision criteria needs to be defined which specifies the minimum thresholds for metrics for a positive go decision to be reached in respect of training controls.

Branch Technology
(Ref. 2017/18-26)

Needs Improvement

Sponsor:
Debbie Smith

Audit actions:

P1	0
P2	4
P3	3
Total	**7**

The Branch Technology project started in 2015 and was initially scheduled to deliver 22,500 counter terminals by June 2018 at a total cost of £49m. Costs have increased by 9% (circa £5m) as a result of an incorrect estimation of the number of terminals required (4,500 shortfall) and licensing costs. The objective of this review was to consider how the overall Branch Technology project is managed and whether it is on track to deliver successfully by September 2018.

Although the project has entered the latter stages of its lifecycle (now in the 26th month out of a proposed 30), there remains a significant volume of deployments outstanding, specifically 62% of counter terminals have not yet been deployed. The project team remains confident that deployments can be completed by September 2018, however, this audit has highlighted that the project is at risk of further cost and delays prior to deployment being completed, with insufficient governance and contingency in place to effectively mitigate these risks. Slippage past October 2018 would result in deployments being paused due to the 'change freeze' commencing in November 2018. If deployments are not completed by March 2019 then Fujitsu will have issues supporting the current application of HNGX beyond this date, resulting in additional costs ranging from circa £0.5m to £1.5m.

Key audit findings:

- There remain areas for improvement in the governance arrangements of the project, including ineffective risk and issue management and unclear roles and responsibilities.
- Delivery to the required timetable requires Computacenter to exceed contractual requirements of deployments per day - if contractual requirements were not exceeded, significant delays would occur.
- The required delivery rate of 80 branches per day at a 95% success rate has not been consistently achieved. Although ongoing monitoring is in place, deployment delivery timeline remains challenging with no contingency.

Business Continuity Management (BCM)
(Ref. 2017/18-17)

Needs Significant Improvement

Sponsor:
Jane MacLeod

Audit actions:

P1	0
P2	6
P3	1
Total	**7**

The objective of this review was to assess the adequacy of the BCM strategy, process and the BC plans as defined, including the design and operating effectiveness of controls in place.

There are areas of good practice in the BCM programme and some progress has been made in rolling out plans since the appointment of the current BC Manager. The BCM Policy is broadly aligned to the international standard (ISO 22301) and there is a high level of engagement from the Board Sponsor and Audit, Risk and Compliance Committee (ARC), who provide programme governance.

However, the review has identified areas where the BCM programme does not yet align to good practice or ISO 22301. Work is required to deliver alignment with the standard, and enable full management oversight of the BCM planning. The review identified a number of areas where work / effort is required. These include:

- There was a lack of visibility of where plans are held and their current status and it was difficult to obtain a clear understanding of the state of the BCM programme through

	documents and records; this may limit governance capability. • Key measures that support the robust and timely delivery of an adequate BCM programme and would enable the champions to deliver robust planning activity, has not yet been achieved. • Planning deliverables based on the current Business Impact Analysis (BIA) template may not provide management with the ability to confirm continuity and recovery prioritisations are correct, nor provide the planners with the focused information needed to deliver streamlined, joined-up BC plans. • PO is not yet exercising BCM plans effectively to assure itself that arrangements and plans that are in place will deliver the outcomes required, or identify areas of weakness. It is also falling short of current contractual exercising commitments expected by third parties. • There is no training material or approach in place to equip individuals across the business to deliver useful business continuity plans.

Reviews in Progress (2017-18 Audit Plan)

7. The following reviews from the 2017-18 audit plan are being finalised:

	Review	Status / Remarks
1	Telecoms Control Framework	Report being reviewed by management
2	Pension Schemes	Report being reviewed by management
3	IT Governance and Risk Management	Report being reviewed by management
4	Back Office Transformation (POLSAP Migration Re-plan)	Report being reviewed by management

Reviews in Progress / Planned (2018-19 Audit Plan)

8. The following reviews from the 2018-19 audit plan are in progress or being planned for delivery in Q2:

	Review	Status	Timing(1)
1	Procurement Fraud Investigation	Fieldwork nearing completion	30/04 - 15/07
2	Product Risk Review – Postal Orders	Draft report	30/04 – 25/06
3	Employee Expenses	Fieldwork	14/05 - 15/07
4	Change Governance Framework (Advisory)	Fieldwork nearing completion	02/05 – 15/07
5	DMB Strategy (Change Assurance)	Fieldwork	25/06 – 31/07
6	Payroll	Scheduled	August
7	Month-end Close Process	Planning	September
8	Cyber Security	Scheduled	September

(1) The timing of the reviews not yet in flight are currently being reviewed in light of the appointment of the new internal audit co-source provider.

Updates on Internal Audit Open and Overdue Actions

9. Following is the status of open and overdue actions:

Audit Action Status at 29 June 2018:	BAU	Change	Total
Open (not yet due)	19	8	**27**
Overdue (<60 days)	0	12	**12**
Overdue (>60 days)	0	0	**0**
Total	19	20	**39**

10. Updates have only been received for two out of the 12 overdue actions and therefore we are unable to provide the reasons for actions being late or revised completion dates. These actions will now be escalated and verbal updates will be provided during the RCC meeting.

Description of action and Priority rating	GE Sponsor	Comments and Action Owners
EUM Programme		
7 actions overdue since 31 May 2108: 1 x P1 2 x P2	Debbie Smith	Updates requested on 1/06, 13/06 and 25/06. Update received from Claire Hurrell only. No updates from Julie Thomas, Esther Harvey and Chirag Kachalia.
Back Office Transition (Lessons to be Learned)		
1 P1 action overdue since 31 May 2018.	Rob Houghton	Updates requested on 1/06 and 13/06 from action owner, Tim White. No response received.
Project Mercury		
4 P1 actions overdue since 31 May 2018.	Debbie Smith	Updates requested on 1/06, 13/06. Update received from Jeff Lewis for his action. No updates received from Karl Oliver for his 3 actions.

END OF REPORT

Appendix 1

2017-18 Internal Audit Plan - Status as at 02 July 2018

No.	Title/Subject	Sponsor	Original / Addition	Timing	Status / Rating
Internal Control Reviews					
1	VAT Process	A. Cameron	Addition	May	Needs Improvement
2	Lottery Prize Pay-out (Design effectiveness)	D. Smith	Addition	August	Satisfactory
3	Financial Spreadsheet Controls	A. Cameron	Addition	August	Needs Improvement
4	IT Control Framework (Advisory)	R. Houghton	Original	March - Aug	Advisory Report
5	Mails Process	D. Smith	Original	July	Satisfactory
6	Information Security (2016) Follow-up review	R. Houghton	Original	September	Needs Significant Improvement
7	IT Security Transformation (Advisory)	R. Houghton	Original	March - Dec	Advisory Report
8	Compliance with Banking Framework	D. Smith	Original	August	Needs Significant Improvement
9	Customer Complaints	A. Cameron	Original	November	Needs Improvement
10	MoneyGram: AML Compliance	J. MacLeod	Original	September	Satisfactory
11	Telecoms Control Framework	O. Woodley	Original	April	Reporting
12	Business Continuity	J. MacLeod	Original	April	Needs Significant Improvement
13	Data Protection (follow up) (GDPR)	J. MacLeod	Original	January	Needs Improvement
14	Pension Scheme(s)	A. Cameron	Original	March	Reporting
15	Financial Control Framework	A. Cameron	Original	February	Satisfactory
16	IT Governance and IT Risk management	R. Houghton	Original	April	Reporting
Change Assurance					
1	SAP SuccessFactors - Payroll	M. Kirke	Original	June	Needs Improvement
2	Integrated Change Plan (Advisory)	R. Houghton	Original	July	Advisory Report
3	IT Networks	R. Houghton	Original	October	Needs Improvement
4	SAP SF Payroll Go-Live Readiness Review	M. Kirke	Addition	December	Acceptable (PwC)
5	SAP SF Payroll Lessons Learnt	M. Kirke	Addition	January	Not Rated
6	Back Office Transition Lessons Learnt	A. Cameron	Addition	January	Not Rated
7	Back Office Transformation - POLSAP to CFS	A. Cameron	Original	March	Reporting
8	Back Office Transformation Cash Processing	A. Cameron	Cancelled	April	Combined with #7
9	Project Solar - HNGT Lite (Prev. Chameleon)	D. Smith	Original	February	Needs Significant Improvement
10	Network Transformation	D. Smith	Original	February	Satisfactory
11	Branch Technology - EUC Transition	D. Smith	Original	February	Needs Improvement
12	EUM	D. Smith	Original	March	Needs Improvement
13	Peer to Peer Encryption Implementation	J. MacLeod	Cancelled		Cancelled

Note: Target audit delivery per original approved plan is for 29 audits (16 internal control reviews and 13 change assurance reviews).

Appendix 2

2018-19 Internal Audit Plan - Status as at 02 July 2018

No.	Title/Subject	Sponsor	Original / Addition	Timing	Status / Rating
Internal Control Reviews					
1	Product Risk Review (Postal Orders)	D. Smith	Original	April	**Reporting**
2	Employee Expenses	A. Cameron / J. Arakji	Original	April	**Fieldwork**
3	Procurement Fraud Investigation	A. Cameron	Addition	May	**Fieldwork**
4	Month-end Close Process	A. Cameron	Addition	Sept	**Planning**
5	Procure to Pay	A. Cameron	Original	Oct	Not Started
6	Payroll	A. Cameron / J. Arakji	Original	Aug	Not Started
7	Branch Cash Forecasting & Management	A. Cameron	Original	Q3	Not Started
8	Cyber Security	R. Houghton	Original	Sept	Not Started
9	Supply Chain Management (Logistics)	A. Cameron	Original	Nov	Not Started
10	Contract Management	A. Cameron	Original	Q3	Not Started
11	IT Control Framework	R. Houghton	Original	Oct	Not Started
12	Client Settlements Process	A. Cameron	Original	Oct	Not Started
13	Digital Strategy & Capability	O. Woodley	Original	Oct	Not Started
14	Whistle-blower Process (Grapevine)	J. MacLeod	Original	TBC	Not Started
15	Agents Remuneration	A. Cameron	Original	TBC	Not Started
16	Financial Control Framework	A. Cameron	Original	Q4	Not Started
Change Assurance[1]					
1	Change Programme Governance	R. Houghton	Original	May	**Fieldwork**
2	Payzone Business Integration	D. Smith / A. Cameron	Original	TBC	Not Started
3	DMB Strategy	D. Smith	Original	July	**Fieldwork**
4	Placeholder - Gold / Platinum Programme	TBC	Original	TBC	Not Started
5	Postmasters Portal	D. Smith	Original	TBC	Not Started
6	Identity Services	M. Edwards	Original	TBC	Not Started
7	Tracked Online/Disintermediation Risk	D. Smith	Original	TBC	Not Started
8	Customer Hub (Additional Verticals)	O. Woodley	Original	TBC	Not Started
9	Banking Framework - Cash Management	D. Smith	Original	TBC	Not Started
10	Project Everest	R. Houghton	Original	TBC	Not Started

[1] The list of Change Assurance reviews was approved by the ARC on the basis of being the highest risk programmes planned for 2018-19 at the time. The list will be reviewed and updated periodically to reflect the programmes most deserving of independent assurance.

Note: Target audit delivery per original approved plan is for 26 audits (16 internal control reviews and 10 change assurance reviews).

POST OFFICE
RISK AND COMPLIANCE COMMITTEE

Compliance Report

Author: Jonathan Hill Sponsor: Jane Macleod Meeting date: 10th July 2018

Executive Summary

Context

In April 2018, Post Office established a new combined compliance function within LRG, comprising Regulation and Compliance for our Financial Services and Telecoms businesses, Financial Crime compliance and Information Protection and Assurance.

It is anticipated that over the near future Compliance will encompass also regulation and compliance for the Banking, Payments, ATMs, Mails and Identity businesses and, working with IT Cyber Security, cyber-crime.

This papers sets out the first consolidated compliance report for Post Office Ltd.

Questions this paper addresses

- What are the regulatory/compliance regimes Post Office operates within?
- What are the key compliance issues and what is the business doing to address these?
- What is the forward-looking regulatory agenda?

Conclusion

The key compliance risk areas are;-

- Compliance with the Money Laundering Regulations and the remediation of Bureau de Change project requirements. We have already been fined by the HMRC for incorrect branch registrations and this area is being closely managed
- PCI DSS Compliance. Our mitigating actions are highlighted in the report. A key risk is compliance is required as part of our contractual commitment to the Banking Framework
- Meeting the future regulatory agenda. There are a large number of items featured in the regulatory appendix and the regulatory discussion continues to evolve. Of particular focus this year are the new General Condition requirements for Ofcom and the Insurance Distribution Directive which both come into effect in October and require substantial work together with other parties and Principals to ensure compliance
- The report below details how we are meeting these requirements

Input Sought

The Committee is requested to note this paper.

Report

What are the principle regulatory/compliance regimes Post Office operates within?

1. Financial Services

- Under the Financial Services and Markets Act (2000), Post Office is the Appointed Representative (AR) for Bank of Ireland UK plc (BoI) and from 1st October 2015, POMS; the latter for insurance. As the AR, Post Office is responsible for first line risk and compliance, working with BoI and POMS as the second line
- This is overseen by the Financial Conduct Authority. Post Office Ltd has direct interaction with the FCA on an annual/twice yearly basis, as part of the FCA's supervision of BoI
- Prudential Regulatory Authority. Post Office Ltd has direct interaction with the PRA on an annual/twice yearly basis, as part of the PRA's supervision of BoI
- Payment Services Regulations (2017) – these regulate how payment services and electronic money are regulated in the UK. The PSRs are the UK's application of the EU's Payment Services Directive II ("PSD2"). They are overseen by the Payment Systems Regulator, which is part of the FCA. Under section 2.15 of the FCA's guidance on PSRs, along with a range of bodies such as banks and building societies, Post Office can provide payment services without the need for further authorisation or registration by the FCA

2. Telecoms

- The telecoms regulatory regime is set out in the UK Communications Act (2003) and is overseen and enforced by Ofcom
- Ofcom applies the standards for telecoms through its General Conditions, which are being revised. The updated conditions will apply from 1st October 2018
- EU Telecommunications Single Market Regulation (2015) – net neutrality. This sets out guidance for providers about the use of their network and the data flowing through them. It also sets out the standards for information to be provided to customers (e.g., internet speeds). This is enforced through the UK's Advertising Standards Authority
- Digital Economy Act (2017) – this gives Ofcom the authority to demand information to be produced by telecoms providers
- Payment Services Regulations (2017) – Telecoms companies are also subject to the PSRs as a result of PSD2. Under PSD2, the purchase of physical goods and services (e.g., gambling sites) through a telecom operator now falls within the scope of the Directive. In order to avoid the risk of exposure to substantial financial risks to payers, only payments under a certain threshold are excluded (€50/£40 per transaction; €300/£250 per billing month). Telecom operators that engage in such an activity must notify PSR on an annual basis that they comply with these limits. The activity will also be listed in the public registers. We are investigating if Post Office's status as set out above applies also to our Telecoms business

Confidential

3. Information Protection

- General Data Protection Regulations (2017) – This is the EU's update on EU Data Protection Directive (1996), harmonising and modernising data protection legislation across the EU
- UK Data Protection Act (2018) – embeds the GDPR into UK legislation
- In accordance with the DPA and GDPRs, Post Office has appointed a Data Protection Officer ("DPO"), Chris Russell. As part of the appointment, the DPO has a direct reporting line through to the Chair of the ARC in very serious cases
- Privacy & Electronic Communications Regulations ("PECR") (2003) – it regulates direct marketing the telecoms industry
- Articles 8 and 10 of the UK Human Rights Act (1998) – it sets guidance on how the State interacts with individual's privacy
- The above are all overseen and enforced by the Information Commissioner's Office ("ICO")
- ISO27001:2013 – this sets the standards for information security systems. This is three year certification and Post Office is assessed by an independent certification body (LRQ) on a six-monthly basis. Post Office's certification is due for renewal in 2019
- PCI-DSS – Payment card standards, set by Visa and MasterCard, enforced by the merchant acquirers. For Post Office this is Global Payments. This is an annual certification, with the security standards increasing year on year. We are independently assessed annually by a Qualified Security Assessor. For Post Office this is Nettitude

4. Financial Crime

- Proceeds of Crime Act (2002). It is the principal legislation for anti-money laundering in the UK. The Act has been amended since 2002, by the Serious Organised Crime and Police Act 2005, the Serious Crime Act 2007 and the Serious Crime Act 2015
- Money Laundering Regulations (2017) – these set the standards by which firms must seek to minimise the risk of money laundering and terrorism financing. Post Office is directly regulated by HMRC as a Money Services Business because of its travel money business

What are the key compliance issues and what is the business doing to address these?

Financial Services and Telecoms (including Banking Framework):

- The key compliance issues are reviewed by Post Office Compliance and its partners at the BoI Customer & Conduct Risk Committee, POMS Joint Compliance Committee, the Banking Framework Security, Compliance and Governance Committee Compliance and the Telecoms Compliance Committee. The key items for each are reported below:

5. BoI/Post Office Customer and Conduct Risk Committee (CCRC)

- The key customer and conduct risks were reviewed at the June CCRC. The Committee reviewed the conduct risk metrics contained in the Post Office Distribution Conduct Risk Dashboards and agreed they were within appetite. The CCRC meets every other month but with papers shared on a monthly basis
- One red metric for out of date literature (out of 12) was reported, which continues to be a challenge, although this has not resulted in material customer detriment. A range of mitigating actions have been implemented including producing a monthly Branch Focus communication, a Network-wide documented FS literature 'spot' check for Postmasters and Branch Managers to complete, which is then available for Network management to review upon visits. Also, the BoI Business Controls Team ("BCT"), together with the Post Office Conduct Compliance team is supporting the Network with literature compliance, as part of their agreed work plan
- However, we have also challenged the product teams to find more effective solutions for providing customers with product information
- Following the CCRC it was agreed that the BCT and Post Office Conduct Compliance teams would review MI in more detail (e.g., Quality of Sales Report and Work.com) to ensure that the BCT focuses its coaching work on the branches/areas of greatest risk
- Post Office Compliance has met with the BoI Vulnerable Customer Project Manager to discuss our respective work plans. We have initiated monthly meetings at a working level to communicate and where appropriate coordinate our efforts

6. POMS/Post Office Joint Customer and Conduct Risk Committee (JCC)

- The key customer and conduct risks were reviewed at the 2nd July JCC. The Committee reviewed the conduct risk metrics contained in the Post Office Distribution Conduct Risk Dashboards and agreed they were within appetite. The JCC meets monthly
- Two red metrics (out of 15) were reported and related to upheld complaints (related to customers not receiving their gift cards as part of the life promotion and is not branch behaviour related) and CRM Easy Life Insurance mystery shopping results, which continue to highlight a lack of conformance with the sales process. To address this VMS issue, additional training has been provided to the CRMs and their supervisors. The product team is looking at making simplification changes to the application process on the CRM tablets

Confidential

7. Additional Conduct Compliance activities

   - The Conduct Compliance team's monitoring of the sale of FS&T products continues to develop ways of working to include the wider areas of compliance such as Information Security and Financial Crime
   - Additional fact finding is being completed to understand how and what training is delivered/received in the non DMB branches in particular WHS branches. Initial feedback is that branches do not regularly go into Horizon to pick up the 'Branch Focus' communication which includes operations updates
   - We are working the Network and L&D teams to build a robust training programme initially to be delivered in directly managed branches, but with the aim to use the content throughout the network

8. Banking Framework Security Compliance and Governance Committee (SCGC)

   - Visa outages on 1st June and the importance of the Post Office network (which experienced an 8-10% uplift in cash demand) and access to cash as an alternative when other distribution fails
   - Partner proposal for an external Audit on controls in framework following the Internal Audit that was recently undertaken was discussed
   - Personal and Business Banking of branches within framework. It was agreed that Post Office should consider whether some form of best practice guidance needed to be considered for how Branches and their assistants could lodge money into their own accounts
   - The SCGC meets on a quarterly basis and reports to the Banking Framework Steering Committee

9. Telecoms Compliance Committee (TCC)

   - This is a new Committee which has been agreed with Fujitsu and will commence in July meeting every 2 months. The focus will be on current and future compliance with regulations. It will monitor progress and change to ensures risks are appropriately managed and there is transparency between us and our suppliers
   - Removal of copper telephony product - Openreach has announced that they will remove WLR (our Homephone copper product) by 2025 and will replace this with alternative fibre products. Alongside these announcements Ofcom are consulting on new guidance for VoIP services which would be costly for Post Office and could result in forcing us to leave the Homephone market. We are lobbying both Ofcom and government accordingly
   - Over the last two months there have been several data breach incidents in the telecoms business, principally as a result of the failure of our keys suppliers to effect proper controls and keep Post Office advised in a timely manner of such breaches. In all cases Post Office acted swiftly to limit the impact on our customers and minimise the business risk. The establishment of the Telecoms Compliance Committee will further strengthen our controls and oversight of the entire telecoms business chain
     - In one case, which Post Office reported to the ICO, we failed to meet the ICO's reporting timelines partly due to a reporting requirement interpretation difference and also due to the late advice from our suppliers. This will result in a fixed monetary penalty notice (£1,000) from the ICO,

which will be published on the ICO's website. In addition we have three similar cases pending, where the supplier failed to notify Post Office in time

10. Customer Hub

- The customer hub went fully live on 20th June with travel money and travel insurance. We have been working closely with the hub team to ensure a compliant delivery
- To this end we are establishing a monthly Enterprise Customer and Compliance Meeting. This Committee will seek to ensure that we obtain appropriate governance and control over tracking these issues whilst ensuring that we still remain part of an agile and digital working environment

Information Protection

11. General Data Protection Regulations ("GDPR")

- The GDPR came into force on 25th May 2018. Post Office delivered its 'effective compliance' programme before this deadline with the one significant exception of contract remediation that was reported to RCC previously
- The Programme has produced its strategy and plan for approval by the GDPR Steerco for 'substantive compliance' with a planned delivery date of the end of November 2018
- Since 25th May Post Office has received in excess of 300 Individual Rights requests, which is approximately 4 times the amount received in the previous year. All of these requests have either been dealt/on track to be dealt with in the statutory timescale of 30 days. The DPO and Head of Portfolio for LRG are monitoring this from a resourcing perspective
- In the first month of the new DP laws Post Office has seen a rise in the number of incidents that are being reported. As yet none of these, other than those within the Telecoms business that have different reporting requirements, have materialised into breaches that are notifiable to the ICO. The GE is kept up to date on all incidents through the weekly Incidents Report

12. PCI DSS

- There are daily progress meetings with Computacenter and twice a week with Fujitsu to ensure they remain on track with the BAU remediation actions
- To put the issues identified by the QSA into context, we believe that our environment has no Data or IT security exposures (as we have a locked down environment with no card data being forwarded from the device), but are issues related to compliance to PCI standards (matters related to monitoring and logging of device incidents). We remain in position to be able to take card payments from branches without our Attestation of Compliance (AoC)
- There are a number change requests that are being challenged by our supplier (Computacenter) and several legal letters have been exchanged on who is liable for costs
- Once our suppliers have implemented the necessary controls our QSA will be able to start its assessment and provide us our Report of Compliance (RoC) and AoC
- We have formalised all issues identified and are proceeding towards compliance with tight project governance. We are providing updates to our

acquiring bank of our progress and to date there have been no fines or additional charges applied and our relationship remains positive. We have been informed that there are a number of steps before fines are issued, with prolonged dialogue with our acquiring bank whereby they notify us of their intention

Financial Crime

13. Compliance with Money Laundering Regulations

- Annual AML/CTF training for Network and back office staff was delivered 4th – 30th May 2018. As at 27th June completion levels were 93.5% for Network and 95% for back office staff
- Non-conformance issues in the Network from 1st May to 22nd June 2018 included 52 incidents identified at 48 branches
  - 18 branches identified were Directly Managed Branches and/or WH Smith Multiples and these have been addressed by the Financial Crime Team and escalated to Network as appropriate
  - 13 branches remain on the non-conformance watch list following the new ID thresholds and will be manually monitored monthly until the new data environment is fully operational
- The volume of suspicious activity reports (SARs) May and June 2018, was stable (c. 258 in May and c. 150 to 22nd June), and reports relating to bureau de change are increasing overall – most of these from internal monitoring rather than branch reports

14. Travel Money & HMRC

- We have written to HMRC to set out our legal interpretation of and approach to Customer Due Diligence and Fit & Proper requirements under the 2017 MLRs and await their written response, however at a meeting on 21st June the Director General advised us that HRMC agreed with our interpretation of the regulations for Customer Due Diligence, removing the need for us to capture copies of customers' ID. However, the DG also advised that HMRC is holding to its reporting requirements for vetting and Fit & Proper, although she agreed that HMRC would be as practical as possible
- The HR Fit & Proper project team is continuing to progress actions as previously agreed with our HMRC supervisor. Significant work is now required to write to all agents to obtain missing information and their self-certification
- During work on the Fit and Proper data, it was identified that a number of branch premises had been registered incorrectly (41 branches with an 'out of scope' branch type) or not de-registered as required (19 branches). These branches will be notified to HMRC as de-registrations, but it was too late to prevent the annual registration fee for these being processed in June
- The Credence universe data environment for bureau de change was transferred to live on 15th June with c52K records which had not been identified during the extended testing phase. These have subsequently been resolved. Transaction monitoring reports are being finalised and will be phased in over the next six months

- eKYC, PEPs and Sanctions capability went live on 22nd June for all transactions over £2k, with results appended to the transaction data in the Credence universe to enable monitoring and investigation as required

15. Financial Crime Risk Assessment current status

- 19 Product Information Packs received in May and June (Mobile Phone Top Ups, Postal Orders, Travel Money Hub, (9)Partner Banking Framework, Bill Payment Pre Paid Cards, Drop and Go, gift Cards, MoneyGram, Bill Payments, Multi-Currency Card and International Payments)
- 14 Financial Crime Assessments completed in May and June (4 initial risk assessments via the assessment tool – Business Cash Encashment, POCA, Amazon Top-Up, Travel Money Hub. 10 full Financial Crime Assessments – Partner Banking Framework, Bill Payment Pre Paid Cards)
- 9 draft Financial Crime Assessments issued to product managers for review and sign-off in May and June (Partner Banking Framework)
- No Product Information packs overdue/7 due in July and August (PaySafe Cash, Amazon Top-ups, POCA, Business Cheque Encashment, Current Accounts, Savings, Bureau de Change)
- No risk assessments overdue/3 due in July and August (Current Accounts, Savings, Bureau de Change)
- PO Insurance products were due for reassessment in May. Thistle Initiatives assessed these last year, however there were no PIPs completed at that time. A workshop was help in May with PO Insurance to assist with PIP completion and we are awaiting receipt

16. Anti-Bribery and Corruption (ABC) update

- No material non-conformance issues to report. Please refer to separate annual Gifts & Hospitality report and annual policy review and assurance paper
- Annual ABC training is due to be rolled out from 27th July 2018

17. Whistleblowing update

- No material non-conformance issues to report. Please refer to separate annual Whistleblowing report and annual policy review and assurance paper

18. Regulatory updates

- The update relating to the Fifth Money Laundering Directive in the January report remains current
- The impact of and response to the recent US withdrawal from the Joint Comprehensive Plan of Action (JCPOA) with Iran is being assessed via UK Finance, UK and EU regulators and governments. There may be consequences in relation to transactions with individuals travelling in Iran. Post Office continues to engage via UK Finance to determine impacts

19. External threats

- The Travel Money Card was subjected to a sustained BIN card number generation attack in May that impacted c. 5,340 cards/customers (c. 97k card authorisations were attempted online). Cards have been blocked and re-issued. FRES is working with the outsource card processing platform provider

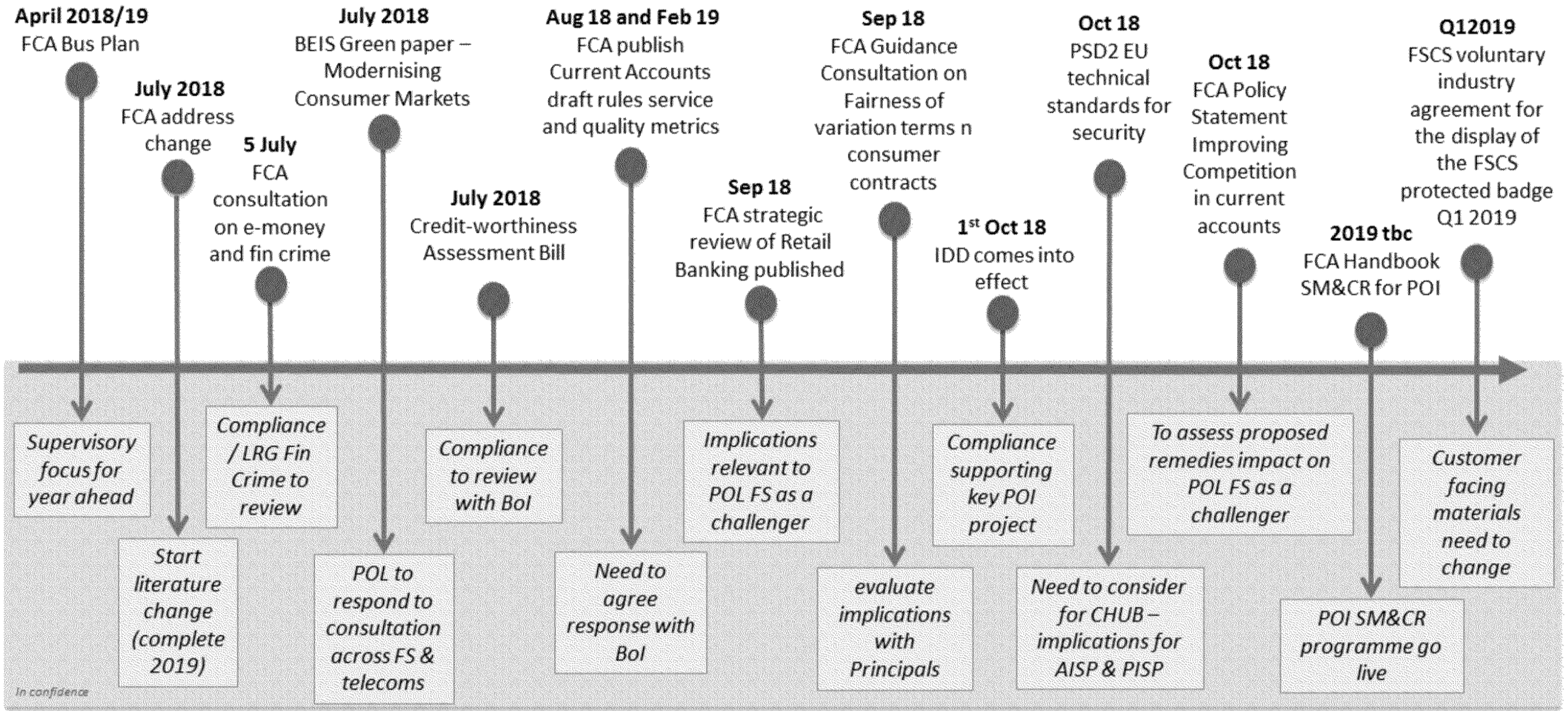
FIS to ensure its authorisation and detection system rules are able to block these type of attacks

- This is not a new style of attack, but illustrates that criminals will exploit known modus operandi and system weaknesses

What is the forward-looking regulatory agenda?

20. The tables below set out the key activities of the Financial Services and Telecoms regulators. As we develop this we will look to include calendars for Financial Crime and Information Security regulation.

Post Office Financial Services Regulatory Calendar



April 2018/19 FCA Bus Plan – *Supervisory focus for year ahead*

July 2018 FCA address change – *Start literature change (complete 2019)*

5 July FCA consultation on e-money and fin crime – *Compliance / LRG Fin Crime to review*

July 2018 BEIS Green paper – Modernising Consumer Markets – *POL to respond to consultation across FS & telecoms*

July 2018 Credit-worthiness Assessment Bill – *Compliance to review with BoI*

Aug 18 and Feb 19 FCA publish Current Accounts draft rules service and quality metrics – *Need to agree response with BoI*

Sep 18 FCA strategic review of Retail Banking published – *Implications relevant to POL FS as a challenger*

Sep 18 FCA Guidance Consultation on Fairness of variation terms n consumer contracts – *evaluate implications with Principals*

1st Oct 18 IDD comes into effect – *Compliance supporting key POI project*

Oct 18 PSD2 EU technical standards for security – *Need to consider for CHUB – implications for AISP & PISP*

Oct 18 FCA Policy Statement Improving Competition in current accounts – *To assess proposed remedies impact on POL FS as a challenger*

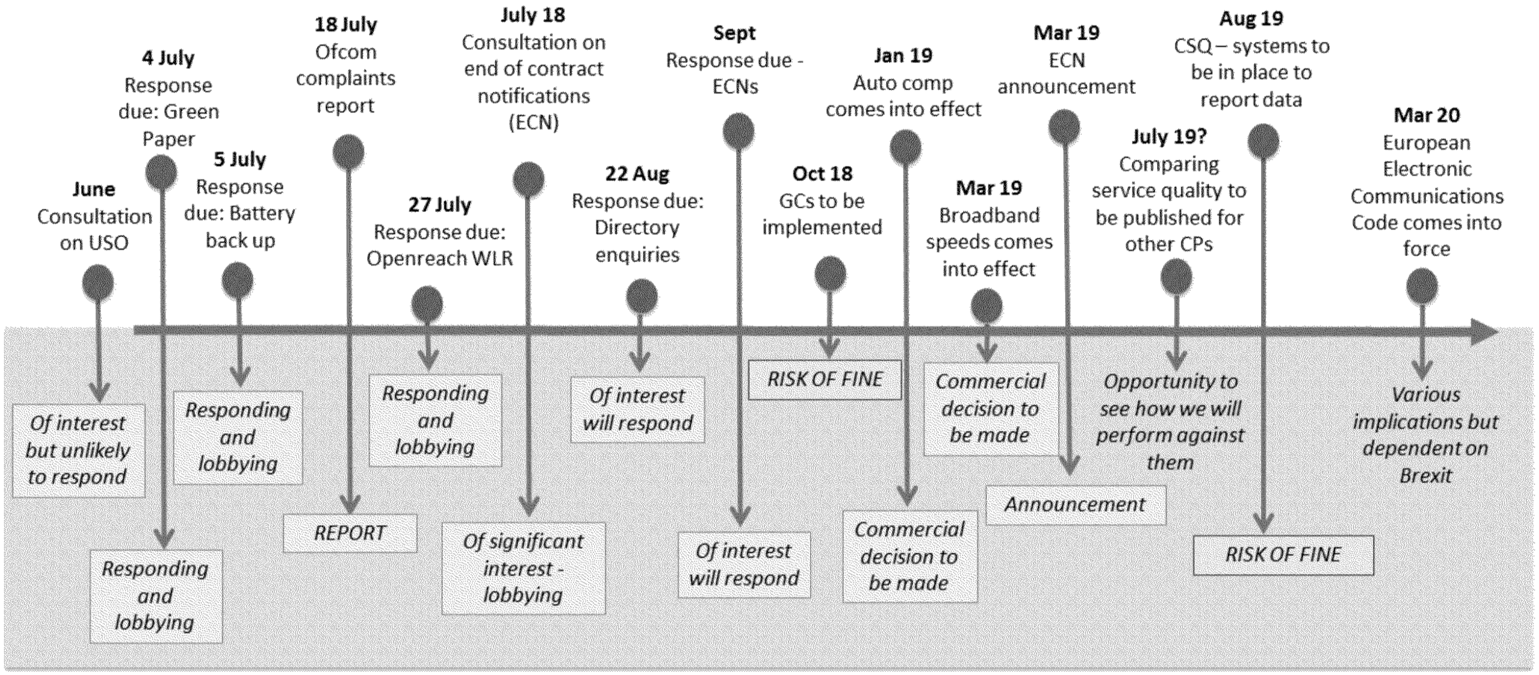
2019 tbc FCA Handbook SM&CR for POI – *POI SM&CR programme go live*

Q12019 FSCS voluntary industry agreement for the display of the FSCS protected badge Q1 2019 – *Customer facing materials need to change*

In confidence

Confidential

Post Office Telecoms Regulatory Calendar



June Consultation on USO – *Of interest but unlikely to respond*

4 July Response due: Green Paper – *Responding and lobbying*

5 July Response due: Battery back up – *Responding and lobbying*

18 July Ofcom complaints report – *REPORT*

27 July Response due: Openreach WLR – *Responding and lobbying*

July 18 Consultation on end of contract notifications (ECN) – *Of significant interest - lobbying*

22 Aug Response due: Directory enquiries – *Of interest will respond*

Sept Response due - ECNs – *Of interest will respond*

Oct 18 GCs to be implemented – *RISK OF FINE*

Jan 19 Auto comp comes into effect – *Commercial decision to be made*

Mar 19 Broadband speeds comes into effect – *Commercial decision to be made*

Mar 19 ECN announcement – *Announcement*

July 19? Comparing service quality to be published for other CPs – *Opportunity to see how we will perform against them*

Aug 19 CSQ – systems to be in place to report data – *RISK OF FINE*

Mar 20 European Electronic Communications Code comes into force – *Various implications but dependent on Brexit*

Confidential

Next Steps

21. We will look to develop a single Compliance dashboard as we develop greater MI capabilities in the business

22. As set out in the introduction, we anticipate that Compliance will encompass also regulation and compliance for the Banking, Payments, ATMs, Mails and Identity businesses and, working with IT Cyber Security, cyber-crime

Jonathan Hill

Compliance Director

July 2018

POST OFFICE

RISK AND COMPLIANCE COMMITTEE

Vulnerable Customers Risk Assessment and Gap Analysis

Author: Jonathan Hill Meeting date: July 2018

Executive Summary

Context

1. The Post Office agreed its Vulnerable Customer Policy in September 2017. This recognised that Post Office is already assisting vulnerable customers in a wide variety of ways reflecting our social mandate.

2. As part of this policy it was agreed that Post Office would undertake a risk assessment during 2017/18. This work was to enable Post Office to identify any gaps in how it supports vulnerable customers and identify good practice.

3. The assessment would also highlight potential solutions in areas where there are gaps identified.

4. We also provided an update and response to the FCA's Ageing Population paper to the Committee in January 2017.

Questions this paper addresses

5. This paper updates the Committee on the assessment. Attached are

- Appendix 1, the assessment,
- Appendix 2 the proposed work plan,
- Appendix 3 the vulnerable customer policy.

Conclusions

6. The overall picture from the review is that Post Office does a huge amount to support customers in a wide variety of vulnerable situations. However, to date Post Office has not been able to present these as a coordinated approach/position.

7. The risk assessment has identified some key required improvements as well as some other items that we could take forward.

8. Key items we are actioning include.

- Required re-organisation and improvement in providing branch literature in an alternative format to vulnerable customers

Strictly Confidential

- Provision of discounted text relay services for Telecoms customers (an Ofcom requirement).
- Compliance with wider Ofcom 'General Condition' rule requirements for vulnerable customers
- Improving our training and awareness of vulnerability across the business
- Reorganisation of vulnerable customer and social responsibility pages on the Post Office website

Input Sought

The Committee is asked for feedback generally and to support the proposed actions in the work plan.

The Report

The Scope of Vulnerability in the UK

9. Significant groups in our communities are impacted either temporarily or permanently by vulnerability. For example;
   - There are 850 thousand people in the UK with dementia and this is expected to rise to a million over the next three years (Alzheimer's Society 2018)
   - In any given year one in four of the adult population suffers a mental illness (NHS 2017)
   - Over 2 million people in the UK are coping with sight loss (RNIB 2015)
   - 6.5 million People in the UK have caring responsibilities. Carers UK predict this will rise to 9m by 2037 (Carers UK 2014)
   - Every 2 minutes someone in the UK is diagnosed with cancer (Cancer Research UK 2014)
   - By 2020 half of the UK can be expected to be diagnosed with cancer at some time in their lives (Macmillan 2014)
   - One in 7 adults has literacy skills of a child aged 11 or below:
   - Just under a half of the population has numeracy attainment skills of a child aged 11 or below (Department of Innovation Business and Skills 2012)

   What is important is that as well as the impact vulnerability has on the individual, the impact spreads widely across family and friends and the wider community who provide care and support to that person.

The Government and Regulatory Context

10. The Government and regulators have put increasing emphasis on ensuring that society does more to ensure that vulnerable customers are protected.

    April 2018 Green Paper issued by the Department for Business, Energy and Industrial Strategy' 'Modernising Consumer Markets'.

    Vulnerability is a key theme in the paper. The Green paper states that '*regulators should act robustly to prevent harm to vulnerable customers and design systems* *that work for vulnerable customers. Companies must understand their customers including those who are vulnerable, and how they can reasonably support their needs'*

One specific area where government wants to see action is in helping consumers with mental ill health, cognitive impairments and dementia including conditions like Alzheimer's'.

11. Ofcom

12. Ofcom has had for some time a number of requirements in relation to vulnerability for example, fault repairs have to give priority to the needs of those with disabilities. These vulnerability requirements have increased following the issuing of the latest regulations (General Conditions) that apply from October 2018.

13. FCA

14. Consumer vulnerability is a key priority for the FCA. As well as the Occasional Paper on Vulnerability that was published in 2015. The FCA's 2018/19 Business Plan states that vulnerability and exclusion will form a key part of their future approach to consumer regulation.

15. The challenges for the vulnerable, the business opportunity and the market response

16. The various regulatory and charity research papers have highlighted the challenges the vulnerable face in accessing goods and services. As well as the obvious physical dexterity and mental challenges; these hurdles can be attitudinal. With the increased number of older and vulnerable members in society together with the support network, getting this right is also an important business opportunity. The vulnerable and the supportive community are customers and potential customers (see below)

17. '*You feel invisible. At the perfume counter the staff ignore me because I am an older woman with a stick. But if I'm with my daughter they are there in a flash. I have the money, I want to buy mascara and make-up but the staff ignore me. They don't think someone like me wants to wear mascara.*' (Female, Newcastle Age UK)

18. The Business Disability Forum 'Walkaway Pound Report' 2015 asked people whether they had left a shop or business because of poor disability awareness or understanding: three quarters (75%) of people with a disability and their families said that they had done this. The forum calculated the headline figure of £1.8 billion per month being lost to businesses that were not disability smart.

19. Vulnerability is an issue our competitors are taking seriously:

- Barclays Bank has focussed on improving the experience for the vulnerable. This includes 'B pay', wearable technology (wristbands, jewellery) to facilitate payments for those that struggle with dexterity, sight problems or dyslexia. As well as clearly signposted support for those with sight, hearing or dexterity problems across the consumer facing business areas. This includes branches giving demonstrations on how to use products and the digital eagles' service to help people get more from the internet.

- BT has a dedicated vulnerability team and a dedicated website ('including you') they undertake roadshows and undertake a regular Consumer Group Forum with vulnerable charities to get feedback on how their services can be improved.

Listening and working with our stakeholders

20. We have engaged with a number of stakeholders to understand the challenges raised by their members and what improvements they would like to see:

- We have engaged with key stakeholders including, Sense, Mind, Alzheimer's Society, Age UK and UK Finance the industry trade association.
- The Alzheimer's Society has reviewed some of our training and we have been in dialogue with the needs of their members. This has included information on the 'Dementia Friends' programme and how Post Office could take part.
- Discussed with the CEO of the NFSP his commitment to vulnerable customers and his support for initiatives such as 'Dementia Friends' and ' Just a Minute (JAM)' cards to enable those who may struggle to communicate to let people know discretely and easily that they just need a little more time.
- We have opened up on an opportunity to work with Sense, together with their accessibility champions to user test the Post Office Customer Hub
- We have joined two relevant industry groups in relation to Financial Services Provision, the Personal Banking Product and Services Board Vulnerability Sub Group and the Financial Inclusion and Capability Working Group to ensure we learn from best practice

How are we meeting the challenge in key areas?

21. Overall the work has shown that we can demonstrate that Post Office takes its responsibilities to vulnerable customers seriously.
22. For example;-

- Numerous examples of community outreach and partnerships with local charities/vulnerable customers made through Agency branches. For example the case featured in the 'Post Office One' with Pontrillas branch that set up a group to combat loneliness and to visit elderly people at home.
- The Banking Framework is a key demonstration of how Post Office is supporting elderly and vulnerable customers. We are increasingly the last 'bank' in town as bank branches close supporting those who prefer to do their banking in branch with the additional support that Post Offices can offer at the counter.
- A Banking process currently exists for DDA/vulnerable customers when they are unable to use the chip & Pin functionality.
- POca serves to meet the needs of the most vulnerable in society including the 'unbanked' and 'financially excluded' through facilitating government payments into a cash account with proprietary card access
- Bill payments operates as a key service for vulnerable customers. In particular the unbanked and those financially excluded. Ability to pay bills via the SSK gives vulnerable customers additional support through trained staff on hand.

23. There are some areas that require immediate action to meet our obligations to the vulnerable which are set out within the next section. We will look to do this within existing budgets where possible.

Key areas-what more we need to do

24. Alternative format literature

25. The provision of alternative format branch literature (e.g., large print, braille, audio) appears to be non-functional in some areas. This has been tested for Credit Cards, Mortgages, Travel Insurance, Home Insurance, Pre Paid Funeral and Telco (Retail is undertaking testing of its products).

26. The test identified that the helpline operators are unaware of the process for supporting these customer needs. This leads to a poor experience for our vulnerable customers and would be looked at critically by our regulators.

27. It is proposed FS&T Compliance will drive a project, working with product managers, and marketing that will;-

- Define what we should offer vulnerable customers in alternative format
- Ensure that we deliver consistent solutions to this, working with third party suppliers as required.

28. Telecoms Text Relay service

A text relay service is used by customers on landlines with communication difficulties. Although we have a text relay service, we are non-compliant as we do not offer discounted rates for this service, which is required by Ofcom. A plan is in place to make these changes working with our supplier, Fujitsu.

29. New Ofcom General Condition Requirements

Ofcom has introduced new requirements for the treatment of vulnerable customers as part of its General Conditions refresh. These regulations come into force in October 2018. We are required to publish a Telecoms Vulnerability Policy on our website.

The new regulations also mean that we have to take into account more transient types of vulnerability e.g. bereavement and divorce. Previously, the regulations were focused on the treatment of customers with disabilities (the provision of discounted text relay and the supply of large print/braille bills).

A work plan is in place to meet the all new General Condition requirements related to vulnerability by the required date of October 2018.

30. Training our staff and the Network (including Dementia Friends)

31. There is some existing guidance in place across the Network as part of the Accessibility Guide 2014 (this has recently been re-reviewed by accessibility consultants see Appendix). The annual compulsory FS workbook and test, also includes a limited learning section/question on vulnerability as well as the Telco training materials.

32. We intend to build on this with a specific module on 'vulnerable customers' on Success Factors that will be available for all our employees.
33. We are also working together with the NFSP on communications and initiatives for our Agents with the Alzheimer's Society-and the 'Dementia Friends' initiative. The Alzheimer's Society materials and the 'Dementia Friends' initiative is something we are considering taking forward as the training messages given (about taking more time, listening etc.) are generic to most vulnerable groups.
34. The Alzheimer's Society will be able to recognise our training as creating Dementia Friends if it meets their criteria and we report back numbers who complete the training regularly.

35. Communication on the Post Office Website

The current vulnerability information is difficult to find on the Post Office website. The existing information needs to be updated as there are some out of date references. One of our priorities is giving better direction and support for the bereavement/Power of Attorney Process. We also need to improve our information on avoiding scams, working together with the BoI.

It is proposed that together with the Marketing and Digital teams, we incorporate the Post office's approach to supporting vulnerable customers in a new social responsibility and community pages, looking to go live August 2018.

Proposed Next Steps and the way forward

Following re-organisation changes, the new co-sponsors of this work are the Network and Sales Director Roger Gale and the Compliance Director Jonathan Hill.

The next steps are to take forward the action plan across the Post Office and continue our work on vulnerability working with our stakeholders where required and continuing to learn about best practice.

Jonathan Hill
Director of Compliance

<u>Vulnerable Customers</u>

Assessment of approach towards 'Vulnerable Customers'

24/06/18

Extract from Post Office Vulnerable Customer Policy September 2017

'By not addressing the needs of vulnerable customers, the impact could be significant for those customers that depend on us to deliver our products and services….It could also cause reputational damage undermining Post Office's achievement of its social purpose. Under both Ofcom and FCA rules there could be regulatory interventions for not treating vulnerable customers fairly.'

Red	Key area that needs resolving and work plan unclear. Prompt resolution required to meet our requirements for customers, non-compliance could have regulatory or reputational impact
Amber	Issues identified and work plan in place, no breach provided actions delivered as planned
Green	No current customer or compliance issues identified but there may be work plans (some significant) to improve our offering/proposition

Vulnerable Customers

Which areas	What we know (how we support customers)	Reg/Legal Regt	Suggested actions	RAG Status	By Who (Owner)
Branch Accessibility	• Branch Accessibility Guidelines. There is a good Network management understanding of the accessibility requirements branches need to adhere to particularly through NT. • There is comprehensive guidance on this provided in a document dated March 2014 covering ;- • Disability and the Equality Act • Post Office's Accessibility Standards and Guidance • Further Sources of Help and Advice • An Accessibility Assessment Form • The assessment of Retail is that this guidance is well understood by the Network Lead Team.	Yes-DDA reqts	We have recently asked our external Accessibility Adviser and our legal team to help us update the guidelines. Once available we need to work with the Communications Team and Network to work through how this should be re-communicated particularly the messages about how to identify and assist vulnerable customers. We are aware the Direct Enquires site (The Nationwide Accessibility Site) does not have up to date information on Post Offices. We are working to update this with our suppliers. Once updated we should link this to Post Office Corporate site.	**Green**	**Martin HopCroft Date Sep 2018** **Network (TBA)** **Network**
Network	Numerous examples of community outreach and partnerships with local charities/vulnerable customers made through Agency branches. For example the case featured in the 'One' with Pontrillas branch that set up a group to combat loneliness and to visit elderly people at home.	No	Work with marketing to see how these good news stories could feature on our website.	**Green**	**FS&T Risk and Marketing (June2018)**

Vulnerable Customers

Which areas	What we know (how we support customers)	Reg/Legal Regt	Suggested actions	RAG Status	By Who (Owner)
Propositions General. Consideration of Vulnerability for new Projects	For some FS products we undertake a Consumer Detriment Risk Assessment (CDRA) to review whether a new or changed proposition or distribution method could have a potential detrimental effect on customers. But it is unclear how this is undertaken for other propositions.	Yes (FCA/Ofcom)	We ensure that as part of our Gating Process there is a step to challenge on whether vulnerable customer requirements are relevant and if so whether they have been considered	**TBC**	**TBC**
Propositions **Mails**	• Although we do not own or control the specifications of our mails products, our supplier, Royal Mail (RM) has a good track record in this area. RM provide: • Literature in braille • Welsh language options • Hard of hearing helpline support • POL acts to signpost these RM services to customers who need them. • RM also has an 'articles for the blind' service. If the recipient of the mail is blind then the sender can post free of charge. This service must be offered as part of the Universal Service Obligation • As part of our contract with RM we must have a least one host to 4	No	From a product perspective there is very little we can change as they belong to RM. Citizens Advice has recently submitted a report for review related to Postal Services. PO to review and consider if there are any lessons learned as a result of this,	**Green**	**James Scutt to review and follow up with mails team**

Vulnerable Customers

Which areas	What we know (how we support customers)	Reg/Legal Regt	Suggested actions	RAG Status	By Who (Owner)
	SSKs. Hosts are not there to specifically help vulnerable customers but are able to offer support if required. Likewise mails transactions are all available over the counter which is an assisted sale. RM also offer a Special Circumstances mails redirection service for those with power of attorney seeking to redirect mail on someone elses behalf. This service is not free.				
Government Services	**POca:** POca serves to meet the needs of the most vulnerable in society including the 'unbanked' and 'financially excluded' through facilitating government payments into a cash account with proprietary card access. The customer base split between 'working age' claimants and 65+ pensioners. The service distributes large volumes of cash through our branch network and serves as a significant part of our social purpose by providing a critical service to the financially excluded. Monthly statements are available in the following formats: • Braille	No	The rollout of Universal Credit (UC) and a changing competitive landscape are the key drivers of change. POca becomes an unsuitable product for customers under UC due to the limited functionality and increased claimant financial responsibility to manage funds, which cannot be supported on the existing product. There has been a shift in the financial services industry targeting the 'unbanked' and 'financially excluded', fuelled by regulation and government policy on Financial Inclusion. The market is evolving with the rise of challenger banks, increased pressure on traditional high	**Amber**	**Ross Borkett** **Pilot Q4** **Launch Q1 2019/20**

Vulnerable Customers

Which areas	What we know (how we support customers)	Reg/Legal Regt	Suggested actions	RAG Status	By Who (Owner)
	• Large print • Audio CD		street banks to provide basic bank accounts and the continued presence of Credit Unions. The Future of POca programme seeks to address the current challenges through the development and delivery of new solutions that will replace the current POca service, better serve our customers and meet the requirements of DWP. The Future of POca programme seeks to achieve the following outcomes: • Maintain and grow the number of financially excluded customers we serve (either directly or through our banking framework). • Continue to drive footfall into our branch network and support the retailer proposition. • Support our wider cash and ATM strategies. • Deliver a sustainable profit.	▨	

Vulnerable Customers

Which areas	What we know (how we support customers)	Reg/Legal Regt	Suggested actions	RAG Status	By Who (Owner)
			• Continue to be one of the main providers of services to the financially excluded while also helping customers avoid the poverty premium.		
Payment Services	**Bill Payments:** Bill payments operates as a key service for vulnerable customers. In particular the unbanked and those financially excluded. Ability to pay bills via the SSK gives vulnerable customers additional support through trained staff on hand. **ATMs:** • Fundamental POca access route to cash outside of POL branch opening times • Mobile phone top ups for PAYG customers • Talking functionality • DDA compliant • Upgraded machines now dispense £10 polymer notes which have braille on them • Mixture of Internal ATMs as well as External machines to help provide additional	**Yes DDA**	**None identified**-Paul Wordsworth and Public Affairs have responded (June 2018) to the Energy UK Commission for Customers in Vulnerable Circumstances. The Commission will be independently chaired, by Lord Whitty and will explore how standards of care and support for vulnerable customers can be improved. The Commission will report by the end of 2018, and make recommendations for industry, Government and other stakeholders. In addition to the work of the Commission, Energy UK will be separately developing a new 'Vulnerability Charter' to build on existing commitments	**Green**	

Vulnerable Customers

Which areas	What we know (how we support customers)	Reg/Legal Regt	Suggested actions	RAG Status	By Who (Owner)
	security/privacy to those who require it • Free to use balance inquiry/mini statement **Non-Cash Payments:** • PACE system in place (the authorisation of transactions via a signature rather than pin pad from other banks. Eg: Lloyds counter cash withdrawal made via card and signature • Full ergonomic assessment of pin pads has been undertaken in relation to supporting people with disabilities: conclusion is that the pin pad is reasonably accessible and usable, although there are issues that have been identified for those with a serious sight issue • Braille on pin pad		and go further to support customers most in need. Our intention through this engagement is to position the Post Office as being a key cornerstone in how the UK Energy Industry supports Vulnerable Energy Customers in paying their bills.		
Identity	**Verify:** Product needs to be improved to provide specific support to aid those customers that are excluded from financial and other services because of the difficulties in passing ID checks.eg the usual passport plus utility bills etc.	No	This is a significant challenge and business opportunity. Delivery road map in place, working with UK Finance and regulators to ensure approach is aligned to industry requirements and there is scope for sharing a central ID standard.	**Green**	**Bryn Robertson Morgan Ongoing Programme through to 2019**

Vulnerable Customers

Which areas	What we know (how we support customers)	Reg/Legal Regt	Suggested actions	RAG Status	By Who (Owner)
	Digital Check and Send: No need to write/take photo/sign etc. Transaction handled by the agent. Photo booths are set up to cater for people with disabilities.				
Banking Framework	The Banking Framework is a key demonstration of how Post Office is supporting elderly and vulnerable customers. We are increasingly the last 'bank' in town as bank branches close supporting those who prefer to do their banking in branch with the additional support that Post Offices can offer at the counter. Banking team are proactively looking to work with Credit Unions, Homeless charities for vulnerable people, where they have no relationship with the mainstream banks. A Banking process currently exists for DDA/vulnerable customers where they are unable to use the chip & Pin functionality. Bank approaches team in Bristol to agree a mandate with the PO branch to make cheque encashment e.g. 3 times a week for £100.	No	Five point plan to promote Banking Framework including enhanced support for vulnerable customers following Citizen's Advice Guidance. FS&T Compliance are working with UK finance on the vulnerability principles to follow working together with CAB	**Green**	**Martin Kearsley- and FS&T Compliance Sep 2018**

POL00401627

Vulnerable Customers

Which areas	What we know (how we support customers)	Reg/Legal Regt	Suggested actions	RAG Status	By Who (Owner)
PO Money products	Post Office Money target customer segments are not age-based but are attitude based and include older customers' needs, particularly in the first two categories of our three target segments (Prosperous and Discerning, Socially Responsible) We have product propositions aimed at older customers, including products for end of life planning (savings, pre-paid funeral, over 50s life, life assurance and home insurance). Our latest product propositions are specifically considering the needs of older customers, including an intergenerational mortgage Post Office Family Link and a freedom mortgage Post Office Retirement Link. The Retirement Link product is specifically designed for those that need to access capital from their home (for example, for later life planning or care costs) without having to sell up or downsize. We are also evaluating savings and lending propositions for those that have cash flow needs including those that may be caring for generations above and below them; or for those that need funds to cover care costs. The regulator has also tacitly acknowledged that its application of	Yes (FCA guidance)	FS&T Risk have recently joined two working groups as part of our membership of UK Finance a Vulnerability Sub Group and the Financial Inclusion and Capability Working Group. We will assess what best practice is in the industry and feed back to FS&T and Post Office as required.	**Green**	**Jonathan Hill ongoing**

Vulnerable Customers

Which areas	What we know (how we support customers)	Reg/Legal Regt	Suggested actions	RAG Status	By Who (Owner)
	regulations (particularly for mortgages) has led to product providers excluding access to older customers for regulatory reasons. In this new climate we are working with BoI on re-evaluating the upper age limit for lending products. Power of attorney process was reviewed and updated in Dec 2016 with support pages on Horizon help (but see below actions)				
BOI supplier of Post Office Money products	BoI has a specific team and programme assigned to vulnerable customers and they are plugged in to industry initiatives. Mandatory training for all BoI staff and additional training for customer facing areas eg call centres. Notifications of bereavements and POA requests are processed by a specialised team. Vulnerability consideration taken into account for premature PO Money bond closure eg divorce, redundancy Unusual levels of withdrawals are monitored and blocked. PO Money Mortgages – specialist team to support customers when faced with	Yes (FCA guidance)	The UK's biggest high street banks and building societies agreed to implement a new set of Principles in line with **'*Easy for friends and family to support*' –** designed to improve processes around the registration and use of legal instruments that can be used to enable third party access to financial affairs such as Power of Attorney, Court of Protection Orders to Appointees and Guardianship Orders. Firms including BoI are targeting March 2019 for implementing changes to their current propositions, where these might not presently meet the minimum standard. The mandate can also be adjusted	**Green**	**PO Money and BoI (March 2019 for third party access initiative)**

Vulnerable Customers

Which areas	What we know (how we support customers)	Reg/Legal Regt	Suggested actions	RAG Status	By Who (Owner)
	~~A~~ arrears, missed payments and a change of circumstances that could impact on the keeping up with the Mortgage payments. Customers are encouraged to act first before going into arrears to prevent impacting on their credit history. PO Money – Credit Cards – letters are sent to customers when the minimum payment is only paid for 6/12 months only explaining the risks.		to describe the minimum proposition for single product providers. This could support friends and family when there is a need to assist or reach out to the bank for help during emergencies such as hospitalisation or other short-term situations of need – all those unplanned circumstances, which might require the assistance of a trusted party to help in paying the bills.		
Post Office Insurance (POMS)	Post Office Insurance has recently put together a high level paper on its approach to vulnerability in an ARC paper. As part of the response it is enhancing call centre training using material from the Alzheimer's Society.	Yes (FCA guidance)	Review FCA feedback statement in Summer 2018 relating to challenges for Firms and consumers in providing and accessing fairly priced cover for people with pre-existing medical conditions for any actions.	**Green**	**Ian Holloway POMS (Sep 2018)**
Travel Money and MoneyGram	Training is given to branch colleagues to help with the identification of 'Scams' for our vulnerable customers for MoneyGram transactions. A number of transfer requests are identified and stopped by branch colleagues, eg September 58 frauds 41% customers were considered vulnerable re Romance scams, a Medical emergency or utility refund.	Yes (HMRC)	Continue to raise awareness of scams on vulnerable customers and good news stories where postmasters have protected them from crime.	**Green**	**Comms team ongoing**

Vulnerable Customers

Which areas	What we know (how we support customers)	Reg/Legal Regt	Suggested actions	RAG Status	By Who (Owner)
Telecoms	Ofcom have introduced new requirements for the treatment of vulnerable customers as part of their General Conditions refresh. These regulations come into force in October 2018 and require us to publish a Vulnerability Policy on our website. The new regulations also mean that we have to take into account more transient types of vulnerability e.g. bereavement, divorce. Previously the regulations were focused on the treatment of customers with disabilities (the provision of discounted text relay and the supply of large print/braille bills). Currently, we identify Elderly and Vulnerable customers ("EVPs") and offer priority fault repair. This process is not comprehensive enough and requires an element of self-identification. We would not categorise someone as vulnerable just because of their age. Telco have undertaken pro-active measures to identify vulnerable customers but further work still needs to be done. For example an initiative to get Care line numbers matched up with Local Authorities help, as a result	Yes (Ofcom)	The Post Office currently only has one category on the system, EVP. New regulations mean that we have to take into account more transient types of vulnerability e.g. bereavement, divorce. We need to be able to tailor our treatment of vulnerable customers according to their needs i.e. not everyone should qualify for free priority fault repair. We also need to ensure that call centre staff have sufficient training to deal with the different categories identified. We need to consider how we should split out customers into different categories so that it's clear if they are "vulnerable" customers and what specific treatment they should receive to meet their needs.	**Amber**	**Meredith Sharples Oct 2018**

Vulnerable Customers

Which areas	What we know (how we support customers)	Reg/Legal Regt	Suggested actions	RAG Status	By Who (Owner)
	of this work an additional 4000 cases were identified. Where someone has currently been recorded as "EVP" they receive: • be-spoke approach to collection cycle for bad debts (exclusion from Dunning process). • Delegated authority process (to help if customer can't respond) • prioritisation for fixes and faults • special treatment for pricing changes (Project Galaxy)		As part of this, we plan to review the training and handling of our vulnerable customers. Following this we need to ensure we have a detailed internal procedural document and a public policy that outlines what we do at a higher level. This will be Teleco specific but should be tied into the wider PO policy. Branch staff should also receive vulnerability training across the network and not just training specific to Telco.		
Telecoms	Although we have a Text Relay service, we are non-compliant as we do not offer discounted rates, and this requires a system change. A CR has been raised and this is being progressed by Fujitsu.	Yes (Ofcom)	Fujitsu are implementing a fix to address the current issue.	**Red**	**Meredith Sharples Need to agree timescales with Fujitsu**
Customer Hub	This important innovation needs to take into account the needs of vulnerable customers. Whilst many	Yes (FCA) WCAG	New customer hub. User testing will includes all kinds of user testing including those	**Green**	**Henk Van Hulle. Sep 2018**

Vulnerable Customers

Which areas	What we know (how we support customers)	Reg/Legal Regt	Suggested actions	RAG Status	By Who (Owner)
	vulnerable groups may be tech savvy, many are not. As at June launch MVP01 is not meeting accessibility standards, however Hub does have a plan in place to address this issue.		that are not tech savvy and testing will seek to get a wide range of ages for testing. Charity 'SENSE' have offered testing resource for the Customer HUB 1. To confirm the accessibility standards we are required to meet for an APP. June 2018 2. To agree timetable to meet these. July 2018 3. To engage Sense in user testing after this. Sep 2018		
Communication	**PO Website** **Web Accessibility:** The Accessibility Consultant for Post Office has confirmed that the general digital accessibility standards are adhered to within PO and with our partners (BOI, FRES, Royal London, Aviva etc.-) The Post Office accessibility standards were written 2008 but they are based on WCAG 2.0 (Web Content Accessibility Guidelines) which are an international standard	Yes WCAG	These standards are being revised this year. We have a consultant working with the committee who are developing the revised guidelines (WCAG 2.1) and as result will feed in any key changes to coincide with them being released which means we should be completely up to date with.	**Green**	**Rob Wemys July 2018**

Vulnerable Customers

Which areas	What we know (how we support customers)	Reg/Legal Regt	Suggested actions	RAG Status	By Who (Owner)
Communication	PO Money has on the website some useful information such as Help with Bereavement page which contains the following contacts; • General Register Office for England and Wales opens in new window • Probate & Matrimonial Office opens in new window • National Association of Funeral Directors opens in new window • Citizens Advice Bureau opens in new window • Money Advice Service opens in new window • StepChange Debt Charity opens in new window • National Debt line opens in new window • Debt Advice Foundation opens in new window • Department Of Work and Pensions opens in new window • HM Revenue & Customs Linked to this page are other areas of support; Redundancy, Divorce & Separation, Caring for others finances.	Yes FCA	• PO Money VC pages hard to find. Liaise with Marketing to align and make visible our VC messages. • Some corrections to bereavement pages required. One of our priorities is giving better direction and support for the bereavement/Power of Attorney Process. We also need to improve our information on avoiding scams, working together with the BoI. • New content pages on avoiding scams to be inserted. • Work with Communications team to assess whether a more fundamental re-organisation of the vulnerability information is required alongside our existing information about community etc	**Amber**	**Andrew Ellis PO Money August 2018** **FS&T Risk to raise with Comms team June 2018.**

Vulnerable Customers

Which areas	What we know (how we support customers)	Reg/Legal Regt	Suggested actions	RAG Status	By Who (Owner)
	Post Office has also • Screen reader on One website • Communication on mental health, wellbeing shared online.				
Communication Network	• One off Network communications have been issued on various issues such as dementia awareness in Branch Focus/Team Talks etc • Scam prevention initiatives working together with Age UK and local Police Forces to prevent vulnerable and elderly customers succumbing to frauds • NFSP have communicated to its network details about vulnerable communities and the work postmasters undertake	No		**Green**	
	Written Materials The communications we make to customers are generally as clear and easy to understand as possible. Working with outside agencies as required.		We are noted by 'Crystal Mark' as being members of the Clear English Scheme. We have not established whether we continue to meet these standards or whether we should display this mark on our communications in different media.	**Amber**	**FS&T Risk to take forward with marketing** **July 2018**
	Written Materials/brochures **Communication Materials**	Yes (FCA)(Ofcom)	FS&T risk will drive a project plan working with product managers, owners.	**Red**	**Product Owners in FS&T and Marketing**

Vulnerable Customers

Which areas	What we know (how we support customers)	Reg/Legal Regt	Suggested actions	RAG Status	By Who (Owner)
	The provision of alternative format (eg large print, braille) appear to be broken for FS&T products. This has been tested for Credit Cards, Mortgages, Travel Insurance, Pre Paid Funeral, Home Insurance and Telco. The helpline numbers are not functional and the process appears broken. Generic Here to Help Leaflet doesn't mention availability of any alternative formats		1. Complete testing on other products to see extent of impact on areas outside of FS&T 2. Define what we are going to offer vulnerable customers in alternative format 3. Ensue that we deliver the consistent solution to this working with third party suppliers as required.	▨	**1. James Scutt July 2018** **2. FS&T Compliance working with Retail/FS&T** **3. TBC**
Training and Awareness	There is existing guidance in place across the Network as part of the Accessibility Guide 2014 The annual compulsory FS workbook and test also includes a learning section/question on vulnerability as well as the Telco training materials. The SF 'Delivering a Great Customer Experience' Module has significant training on Vulnerable Customers. Customer Relationship Managers CRMs are trained on vulnerable customers and provided with back up material in paper format for customers	Yes (FCA) (Telco)	We have asked Alzheimer's Society for feedback on our existing training We are considering further training options both through Success Factors for our employees and through alternative methods to our Agents. The Alzheimer's Society materials and the 'Dementia Friends' initiative is something we are considering taking forward as the training given is generic to most vulnerable groups. Design , build and roll out a bespoke VC training module, L & T team have been engaged	**Green**	**FS&T Risk to take forward with Training** **July 2018**

Vulnerable Customers

Which areas	What we know (how we support customers)	Reg/Legal Regt	Suggested actions	RAG Status	By Who (Owner)
	that can't relate to tablet technology. CRM training covers VCs.		and are carrying out this work stream to be delivered into the business in parallel to the new web architecture launch. (key sections will be POA, Probate & Bereavement) **Suite of Videos –** 5 Available, the 'reading and writing' module was filmed within a Post Office. Branch can register on website, receive a unique code which can be watched either individually or as a team. Information can be provided via post codes of where they are being used and who has taken the training. We are also working together with NFSP on communications and initiatives for our Agents with the Alzheimer's Society- and 'Dementia Friends' this initiative is something Royal Mail currently participates in. Any new module in Success Factors to be made available to CRMs as part of Compliance training.	▨	

Vulnerable Customers

Which areas	What we know (how we support customers)	Reg/Legal Regt	Suggested actions	RAG Status	By Who (Owner)
Customer Insight and Experience	Insight team receive feedback from around 1300 customer survey responses per month, within the advocacy programme. Identification of any customer vulnerabilities would be acted upon but none known as time of review.	**No**	**None identified**	**Green**	
NBSC	Jane Smith and Lisa Cawthorne who look after calls from the branch network (NBSC). Product specific issues are directed to the 'Here to Help' leaflet Where customers have access issues reported e.g. wheelchairs, they make local arrangements with the Branches, and by using the branch doorbell to make the branch aware they require assistance. Branches do refer/report any physical branch changes requirements, through the management line.	**No**	To make additional VC training available to NBSC through Success Factors. We will do this by sharing our new VC bespoke training module.	**Green**	**FS&T Risk to take forward with marketing** **July 2018**
Social Media	Our Social Media team has confirmed from a monitoring tool perspective that our system picks up vulnerability buzzwords, and prioritises those posts (aka shows them higher up the queue so they get a faster response time). The Lithium will pick up things that were directly posted onto Facebook,	**No**	**None identified**	**Green**	

Vulnerable Customers

Which areas	What we know (how we support customers)	Reg/Legal Regt	Suggested actions	RAG Status	By Who (Owner)
	twitter, LinkedIn etc. However, if these posts have been made in internet forums, we don't get sight of them. Lisa Cawthorne and Jane Smith have confirmed, once escalated, the Social team respond to the tweets and posts. They will request information to be sent them via email to ensure a full resolution of the issues. They will refer to proposition manager within PO/BOI/POMS, where applicable.				
Complaints	Whilst individual complaints/feedback relating to vulnerability are taken forward it is unclear whether we undertake any trend analysis and learn from them, this is also the case from complaints dealt with by Post Office, BoI. POMS or elsewhere.	Yes-FCA (DISP) Ofcom	Undertake complaints assessment to review whether any more work can be undertaken both through Post Office and third parties to review trends we can learn from.	**TBC**	FS&T Compliance to drive some further exploratory work to assess whether we can do more to learn from our complaints **TBC 2018**
Branch and Staff guidance on how (or whether) to approach the authorities where we are concerned for customers in different circumstances	There have been some occasions when it has been unclear what the protocol should be(if any) for alerting the authorities to protect a vulnerable customer (for example an individual that continually tried to deposit and withdrew tiny amounts of cash from a non-serviced account and was acting confused when help was being offered).	No	Work further with Charity sector to understand practicalities of this. If guidance can be provided we will work this Comms team.	**TBC**	FS&T and Public Affairs to drive some exploratory work on this with our Charity contacts **TBC 2018**

Vulnerable Customers

Which areas	What we know (how we support customers)	Reg/Legal Regt	Suggested actions	RAG Status	By Who (Owner)
e.g. customers with mental illness, or those that are subject to protection orders etc					

Vulnerable Customers work plan

Summary Vulnerable Customer work plan.

This does not cover items already planned to take place as part of our strategy or business planning (eg such as the Identity Programme or the future of POCa work).

This is divided into

1. Work we have to do for regulatory or key stakeholder management.

2 Optional work-nice to haves

3. Challenging things

Vulnerable Customers work plan

1.What we have to do (for regulatory or key stakeholder management).

Which areas	Summary Detail	Reg/Legal Regt	Work plan	Is there a budget consideration?	By Who (Owner)
Branch Accessibility	- Branch Accessibility Guidelines. In place but need updating (2014)	Disability and the Equality Act	Accessibility Adviser has given us feedback on the guidelines. Once available we need to work with the Communications Team and Network to work through how this should be re-communicated particularly the messages about how to identify and assist vulnerable customers. We are aware the Direct Enquires site (The Nationwide Accessibility Site) does not have up to date information on Post Offices. We are working to update this with our suppliers. Once updated we should link this to Post Office Corporate site.	**None expected for the assessment work, TBC for any required changes.**	**Martin HopCroft Date July 2018**
Banking Framework	A key part of the Five point plan to promote Banking Framework includes enhanced support for	Yes-FCA (PSRs)	Post Office is working with UK Finance to agree general	**No budget issues**	**Martin Kersley-Paul Beaumont Sep 2018**

Vulnerable Customers work plan

Which areas	Summary Detail	Reg/Legal Regt	Work plan	Is there a budget consideration?	By Who (Owner)
	vulnerable customers following Citizen's Advice Guidance.		vulnerability principals to be followed.		
Telecoms	Ofcom _new vulnerable customer requirements October 2018	Yes (Ofcom)	The Post Office currently only has one category on the system, EVP. New regulations mean that we have to take into account more transient types of vulnerability e.g. bereavement, divorce. We need to be able to tailor our treatment of vulnerable customers according to their needs i.e. not everyone should qualify for free priority fault repair. We also need to ensure that call centre staff have sufficient training to deal with the different categories identified. We need to consider how we should split out customers into different categories so that it's clear if they are "vulnerable" customers and what specific treatment they		**Meredith Sharples Oct 2018**

Vulnerable Customers work plan

Which areas	Summary Detail	Reg/Legal Regt	Work plan	Is there a budget consideration?	By Who (Owner)
			should receive to meet their needs. As part of this, we plan to review the training and handling of our vulnerable customers. Following this we need to ensure we have a detailed internal procedural document and a public policy that outlines what we do at a higher level. This will be Telco specific but should be tied into the wider PO policy. Branch staff should also receive vulnerability training across the network and not just training specific to Telco.		
Telecoms	Although we have a Text Relay service, we are non-compliant as we do not offer discounted rates, and this requires a system change. A CR has been raised and this is being progressed by Fujitsu.	Yes (Ofcom)	Plan in place to address the current issue.	**None expected**	**Meredith Sharples** **Need to agree timescales with Fujitsu**
Communication	**PO Website**	Yes WCAG	These standards are being revised this year. We have a	**Not known**	**Rob Wemys** **July 2018**

Vulnerable Customers work plan

Which areas	Summary Detail	Reg/Legal Regt	Work plan	Is there a budget consideration?	By Who (Owner)
	Web Accessibility: The Accessibility Consultant for Post Office has confirmed that the digital accessibility standards are adhered to within PO and with our partners (BOI, FRES, Royal London, Aviva etc.-) The Post Office accessibility standards were written 2008 but they are based on WCAG 2.0 (Web Content Accessibility Guidelines) which are an international standard.		consultant working with the committee who are developing the revised guidelines (WCAG 2.1) and as result will feed in any key changes to coincide with them being released.		
Communication	PO Money website requires significant updating on social responsibility and vulnerability	Yes FCA	• PO Money VC pages hard to find. Liaise with Marketing to align and make visible our VC messages. • Some corrections to bereavement pages required. One of our priorities is giving better direction and support for the bereavement/Power of Attorney Process. • We also need to improve our information on avoiding scams,	**Within existing budgets**	**Andrew Ellis PO Money Sep 2018**

POL00401627

Vulnerable Customers work plan

Which areas	Summary Detail	Reg/Legal Regt	Work plan	Is there a budget consideration?	By Who (Owner)
			working together with the BoI. • New pages on avoiding scams to be inserted. • Work with Communications team to assess whether a more fundamental re-organisation of the vulnerability information is required alongside our existing information about community etc. • Work with Comms to see how all these good news stories from the Network could feature on our website.		
	Written Materials/brochures **Communication Materials** The provision of alternative format (eg large print, braille) appear to be broken for FS&T products. This has been tested for Credit Cards, Mortgages, Travel Insurance, Pre Paid Funeral,Home Insurance and Telco. The helpline numbers are not	Yes (FCA)(Ofcom)	FS&T Compliance will drive a project plan working with product managers, owners. 1. Close testing on other products to see if these impact on other areas outside of FS&T 2. Define what we are going to offer vulnerable customers in alternative format	**Yes, to be determined by solution that needs to be put in place.**	**Product Owners in FS&T and Marketing** **July 2018**

Vulnerable Customers work plan

Which areas	Summary Detail	Reg/Legal Regt	Work plan	Is there a budget consideration?	By Who (Owner)
	functional and the process appears broken. Generic Here to Help Leaflet doesn't mention availability of any alternative formats		3. Ensue that we deliver the consistent solution to this working with third party suppliers as required.		
Training and Awareness	To improve our vulnerable customer training across the network. 1. For our employees via a new SF module 2. For the wider Network through initiatives with the NFSP	Yes (FCA) (Telco)	1. Plan in place for FS module 2. We are also working together with NFSP on communications and initiatives for our Agents with the Alzheimer's Society- and 'Dementia Friends' this initiative is something Royal Mail currently participates in.	**Within existing budget**	**L&D Sep 2018**

2. Optional work-nice to haves

Which areas	Summary Detail	Reg/Legal Regt	Work plan	Is there a budget consideration	By Who (Owner)
Proposition (Gating)	To consider vulnerability in all our customer facing propositions	Various eg DDA, FCA, Ofcom etc	Review whether the gating process should include as part of the 'gate' customer vulnerability considerations before new projects go live	**Yes- Potentially depending on any proposition changes to accommodate**	**Paul Beaumont FS&T Compliance Sep 2018**

Vulnerable Customers work plan

Which areas	Summary Detail	Reg/Legal Regt	Work plan	Is there a budget consideration	By Who (Owner)
				vulnerable customers	
Customer Hub	To meet industry best practice for accessibility. Then for this to be tested by the charity Sense.	Yes (FCA) WCAG	This has been factored into MVPO1 post launch	**Within CHUB budget**	**Henk Van Hulle** **July 2018**
Communication material	We are noted by 'Crystal Mark' as being members of the Clear English Scheme.	No	We have not established whether we continue to meet these standards or whether we should display this mark on our communications in different media.	**Not known**	**FS&T Compliance to take forward with marketing** **July 2018**

3. Challenging things

Branch and Staff guidance on how (or whether) to approach the authorities where we are concerned for customers in different circumstances e.g. customers with mental illness, or	Social responsibility. There have been some occasions when it has been unclear what the protocol should be (if any) for alerting the authorities to protect a vulnerable customer if we are concerned about their welfare. (Whilst if someone exhibits threatening behaviour or is threatening their own life there are obvious actions to take relating to contacting the police)	No	Work further with Charity sector to understand practicalities of this. If guidance can be provided we will work this Comms team.	No expected budget implications	LRG Compliance and Public Affairs to drive some exploratory work on this with our Charity contacts **Sep 2018**

those that are subject to protection orders etc					
Complaints	Whilst individual complaints/feedback relating to vulnerability are taken forward it is unclear whether we undertake any trend analysis and learn from them, this is also the case from complaints dealt with by Post Office, BoI. POMS or elsewhere.	Yes-FCA (DISP) Ofcom	Undertake complaints assessment to review whether any more work can be undertaken both through Post Office and third parties to review trends we can learn from.	No budget currently for this activity	A start would be for LRG Compliance to drive some further exploratory work to assess whether we can do more to learn from our complaints **Aug 2018**

Vulnerable Customer Policy

Version – Final 1.0

Group Oversight Committee:	Audit and Risk Committee
Sign-off Authority:	Risk and Compliance Committee
Policy Sponsor:	Kevin Gilliland and Nick Kennett
Policy Owner:	Tom Weschler and Jonathan HIll
Policy Author:	Paul Beaumont and Jonathan Hill
Approved by:	
Approved:	25.09.2017
Next review:	25.09.2018

1. Overview

1.1. Introduction by the Policy Owner

At the Post Office we are committed to providing quality products and services for all our customers. We work in an open and responsible way that builds the trust and respect of all our customers. Post Office seeks to ensure that all customers are provided with good product and service choices, so that they can make good buying decisions and have a positive experience when dealing with us.

Addressing the needs of vulnerable customers is core to Post Office's social purpose and is aligned to our objectives to be 'Better for Customers' and a 'Great Place to Work'. There are countless examples of how we assist customers when they need us most. This policy outlines the policy approach so that we continue to ensure that we are able to look after the needs of vulnerable customers.

1.2. Purpose

To articulate Post Office's expectations as to how employees and agents identify and help vulnerable customers during their interaction with the Post Office its products and services. This will also be an important document and source of information on Post Office's policy approach for many of our stakeholders.

1.3. Core Principles

Much of consumer protection legislation is underpinned by the notion of the average or typical consumer, and what they might expect, understand or how they might behave. Some consumers may be significantly less able to represent their own interests, and more likely to suffer a greater risk of customer detriment than the average consumer, with regard to achieving the most appropriate price, service, product or quality available to them. This may be for a variety of reasons, as outlined below (this list is not exhaustive).

Vulnerability can impact in many ways and these categories are examples. The Post Office recognises that these customers may have additional needs and may be described as 'vulnerable' although it is important to note that these customers may not regard themselves as such. It is core to Post Office's rationale and purpose to ensure that appropriate respect and care is taken of all types of customer, including vulnerable customers.

Categories include:

A. Restricted Mobility B. Communications Needs C. Low Basic Skills D. Low Financial Capability	E. Mental Capacity F. Age Related Vulnerability G. Life Event Vulnerability e.g., bereavement, critical illness, redundancy H. Financial Difficulties

1.4. Application

There are already many examples of how Post Office assists vulnerable customers these include:

- Improving disabled access and fitting hearing loops
- Team talks on vulnerability
- Financial Services and Telecoms training on vulnerability e.g., "Delivering a Great Customer Experience", "General Compliance" training modules and the "Compliance Training Manual for Broadband and Phone"
- Training on mental health awareness risk
- Participation in National Police initiatives to mitigate frauds on vulnerable customers
- Rolling out the Banking framework to ensure financial access to communities including the vulnerable when bank branches are closing
- Our response to the Grenfell Tower fire and ensuring we could support customers in time of emergency
- Working with partners such as BoI who give case by case exceptions to the 'terms of conditions' for customers, for example customers in hospital unable to read banking correspondence and statements, or those that have suffered a bout of mental illness.

Post Office provides advice and guidance to customer-facing staff and those involved in the design of products and services and the processes that support their distribution and sale, regarding the legal requirements, regulatory guidance and relevant industry body recommendations, as well as Post Office recommended best practice.

It is the responsibility of those staff to ensure that they comply with and observe those requirements or guidance, and where there is any uncertainty, to seek clarification from relevant Post Office subject matter experts.

1.5. Risk

By not addressing the needs of vulnerable customers, the impact could be significant for those customers that depend on us to deliver our products and services. These risks are included in the minumum control standards section below but could include customers not being able to access our products or services, inappropriate purchases and not being able to understand the features or terms and conditions of a product or service.

It could also cause reputational damage undermining Post Office's achievement of its social purpose. Under both Ofcom and FCA rules there could be regulatory interventions for not treating vulnerable customers fairly.

1.6. Legislation

- Ofcom duties under the Communications Act

- Disability Discrimination Act 1995
- Equality Act 2010
- Mental Capacity Act 2005 and guidance
- Power of Attorney Act 1971
- Disability Discrimination Act (Northern Ireland) 2005.
- Adults with Incapacity (Scotland) Act 2000.
- Consumer vulnerability regulation detailed within the FCA Handbook for CONC and Mortgage Conduct of Business (MCOB).

1.7. Industry Guidance

- FCA website including 2016 Thematic Review on vulnerable customers
- ABI/BBA Codes of Practice
- Age UK advice line
- Money Advice Service
- Pensions Advisory Service

2. Risk Appetite and Minimum Control Standards

2.1. Risk Appetite

A Risk Appetite is the extent to which the Group will accept that a risk might happen in pursuit of day to day businesses transactions. It therefore defines the boundaries of activity and levels of exposure that the Group are willing and able to tolerate.

Post Office's risk appetite is **averse** for:

- non-compliance with law and regulations or deviation from its business conduct standards, and
- for taking risks which might result in failure to maintain the service commitment in respect of customers in line with our social purpose and Government's policy on subsidy.

The Group acknowledges however that in certain scenarios even after extensive controls have been implemented a product or transaction may still sits outside the agreed Risk Appetite. In exceptional circumstances a Risk Exemption waiver may be granted.

2.2. Policy Framework

Post Office's Board has overall responsibility for ensuring that Post Office has a framework to ensure compliance with legal, regulatory and contractual requirements. The Board is kept abreast of relevant matters relating to the management of vulnerable customer matters by reports from its committees including its Audit and Risk Committee.

It is the responsibility of the policy owners to review this policy at least once a year and on an ad hoc basis as necessary to ensure the policy remains effective and up to date.

This policy will be reviewed by The Post Office Risk and Compliance Committee at least once each year from the last date this policy was determined effective.

2.3. Who must comply?

Compliance with this policy is mandatory for all Post Office employees. We will work with our Agency network, Principals and key commercial partners to ensure that where we can the spirit of our approach to vulnerable customers is applied.

2.4. Minimum Control Standards

A minimum control standard is an activity which must be in place in order to manage the risks within the defined Risk Appetite statements contained within the table below. To comply with this, mechanisms must be in place within each business unit or product to demonstrate compliance. The minimum control standards can cover a range of control types, i.e. directive, detective, corrective and preventive which are required to ensure risks are managed to an acceptable level and within the defined Risk Appetite.

The minimum control standard for the vulnerable customer policy is 'directive' and will be communicated to staff through staff communications and intranet.

We should maintain the existing training requirements that we have in place (for example this is covered in the annual Horizon FS handbook training, Team Talks and the 'Delivering a Great Customer Experience module' on Success Factors) and aim to build on this where we can to ensure that our approach is regularly communicated.

The table below sets out some of the key relationships between identified risk, the considered Risk Appetite, and the required minimum control standards:

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible
Physical access to the branch network is difficult	**A) Restricted Mobility** A customer may be particularly vulnerable because they have mobility restrictions; this means that it might be difficult for them to gain physical access to our premises.	• We will seek to, where it is possible to do so, make 'reasonable adjustments' to our business premises to allow customers with mobility restrictions to access our business premises. • Where we are not able to make such adjustments we will seek, where it is reasonable to do so, to provide the customer with an equivalent service through other means.	Kevin Gilliland / Al Cameron
Customer engagement with products and services is not possible or limited because of a vulnerability	**B) Communications Needs** A customer may be particularly vulnerable because they have a hearing or sight impairment, which means they require specially adapted methods of communication.	• We will look to make 'reasonable adjustments' to the way in which we are able to communicate with our customers. For instance for sight impairment, we will seek to ensure that our customer documentation is available in a range of formats to help them understand our product material and product-life cycle communications • For hearing impairment, we will seek to provide hearing loops, and for our telephony staff, training in use of telephone relay technology.	Kevin Gilliland / Nick Kennett Al Cameron / Kevin Gilliland
	C) Low Basic Skills A customer may be particularly vulnerable because they have a low level of basic skills (including not having English as a first language) and therefore require additional or specialised assistance to effectively make use of our products and	• We will seek to work positively and constructively with customers that have, or appear to have, a low level of basic skills. • We will seek to ensure that the use of jargon is minimised within our documentation. Where it is used we aim	Kevin Gilliland / Nick Kennett

	services or, during the course of the product life-cycle, interact with us and manage their financial position effectively.	to ensure that there is an easy to understand explanation of the term. • We will look to provide sign-posting to free independent sources of information and support that the customer can access in relevant documentation and sections of our websites. • We will seek to explore how to simplify the information that we provide to customers, for example, through the standardised terms and conditions to highlight parts that matter. If appropriate we will engage with government and industry initiatives	
	D) Low Financial Capability A customer may be particularly vulnerable because they have a low level of financial capability (e.g. a specific lack of the maths skills and knowledge of financial products or matters) and therefore may require more straight-forward explanations.	• We aim to be clear and fair and not misleading in communications with customers, and wherever possible we will seek to avoid 'jargon'. We will strive to explain our products and services, including associated risks to customers, in a manner which is easily understandable. • We will seek to take reasonable steps to ensure there is sufficient 'sign-posting' across our product and service proposition to charities and other not-for-profit organisations that provide independent advice and guidance on financial issues	Kevin Gilliland / Nick Kennett
	E) Mental Capacity A customer may be particularly vulnerable because they have a mental capacity limitation (for instanced dementia, a learning disability, a development disorder,	• Be aware of the Power of Attorney requirements where applicable (refer to Horizon Help) • We aim in our dealings with a customer who we know, or reasonably suspect has	Kevin Gilliland/ Nick Kennett

	a neurological disability) that may restrict their ability to appropriately engage with us or make an informed and responsible borrowing decision.	a mental capacity limitation, to act sympathetically and positively. • We seek to allow a customer sufficient time to weigh-up the information and explanations we have provided and defer a decision to a later date. We will seek to provide all the information required to enable a customer to do this. Where possible we should ask if the individual would like to consider this decision with a family member or trusted person.	
	F) Age Related Vulnerability A customer may be particularly vulnerable as a consequence of the effects aging can have on an individual; this includes potential memory loss, dementia or the potential for the customer to be 'overwhelmed' by a particular situation.	• Be aware of the Power of Attorney requirements where applicable (refer to Horizon Help) • Post Office should not automatically assume that a customer is vulnerable by virtue of their age. We seek to provide appropriate products and services to customers of different ages. However, it is appropriate in some circumstances to explain clearly risks which relate to ageing customers e.g., for end of life planning products. • We aim in our dealings with a customer who we know, or reasonably suspect has a mental capacity limitation, to act sympathetically and positively. • We seek to allow a customer sufficient time to weigh-up the information and explanations we have provided and defer a decision to a later date. We will provide all the information required to enable this. • Where possible we should ask if the individual would like to consider this	Kevin Gilliland / Nick Kennett

		decision with a family member or trusted person.	
	G) Life Event Vulnerability A customer that has or is experiencing a specific adverse 'life event' (for example, redundancy, a bereavement, critical or terminal illness, or a marriage breakdown) could be particularly susceptible to making poor judgements. (Although these triggers may not always have a negative impact on the individual)	• We should aim to treat these customers fairly and with a level of sympathy and positivity. We aim to ensure, throughout our businesses, that when we become aware of these life events we have the ability to respond flexibly and deliver an outcome that is appropriate.	Kevin Gilliland / Nick Kennett
	H) Financial Difficulties Customers that are in financial difficulties (for instance high levels of debt or low levels of income) may be particularly vulnerable to financial detriment.	• Be conscious of customers in financial difficulties when designing or introducing products and services that require a regular financial commitment • Be able to manage expectations e.g., declines or alternate payment methods if applying for a product or service • Where feasible signpost Money Advice Service, Citizen's Advice Bureau, Pensions Advisory Service and/or other similar independent advice/helplines	Kevin Gilliland / Nick Kennett

3. Where to go for help

3.1. Additional Policies

This policy is one of a set of policies. The full set of policies can be found at:

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

3.2. How to raise a concern

Any Post Office employee who is concerned about the application of this policy should:

- Discuss the matter fully with their Line Manager; or,
- Report their concerns to the policy owner.
  If you wish to do this anonymously you should contact the 'Speak Up' line on GRO

3.3. Who to contact for more information

If you need further information about this policy, please contact Tom Weschler or Jonathan Hill

3.4. Company Details

Post Office Limited registered in England and Wales. Registered numbers 2154540. Registered Office: Finsbury Dials, 20 Finsbury Street, London EC2Y 9AQ.

Post Office Limited is authorised and regulated by Her Majesty's Revenue and Customs (HMRC), REF 12137104. Its Information Commissioners Office registration number is Z4866081.

Version Control

Date	Version	Updated by	Change Details
July 2017	Draft 0.1	Jonathan Hill / Paul Beaumont	1st draft in revised template
11th July 2017	Draft 0.2.1	Jonathan Hill / Paul Beaumont	2nd draft in revised template
26 Sep 2017	Final 1.0	Paul Beaumont	Approved by ARC on 25/9/2017

POST OFFICE
RISK & COMPLIANCE COMMITTEE

Page **1** of **12**
POLICY REVIEW

6.2 Procurement Compliance Reporting

Author: Barbara Brannon Sponsor: Al Cameron Meeting Date: 10 July 2018

Executive Summary

Context

As a business in receipt of public funds POL is bound by the Public Contract Regulations (2015). PCR 2015 oblige POL to behave in a fair, objective & transparent way when contracting with 3rd party suppliers. Additionally, set procedures must be followed for spend above £25k and £181,302 (total contract value, increased from £164,500 in 2018).

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

The PCR Compliance Register allows for the tracking of breaches to PCR regulations at the Post Office and internal governance processes. One aim of collating this information is to drive improvement in awareness and compliance behaviour across the organisation. The second and primary aim is to work with GE and Business Units to commence commercial reviews in a more timely way ensuring POL obtains value, commercial and contractual flexibility fitting the requirements and business strategy of the organisation.

Questions addressed in this paper

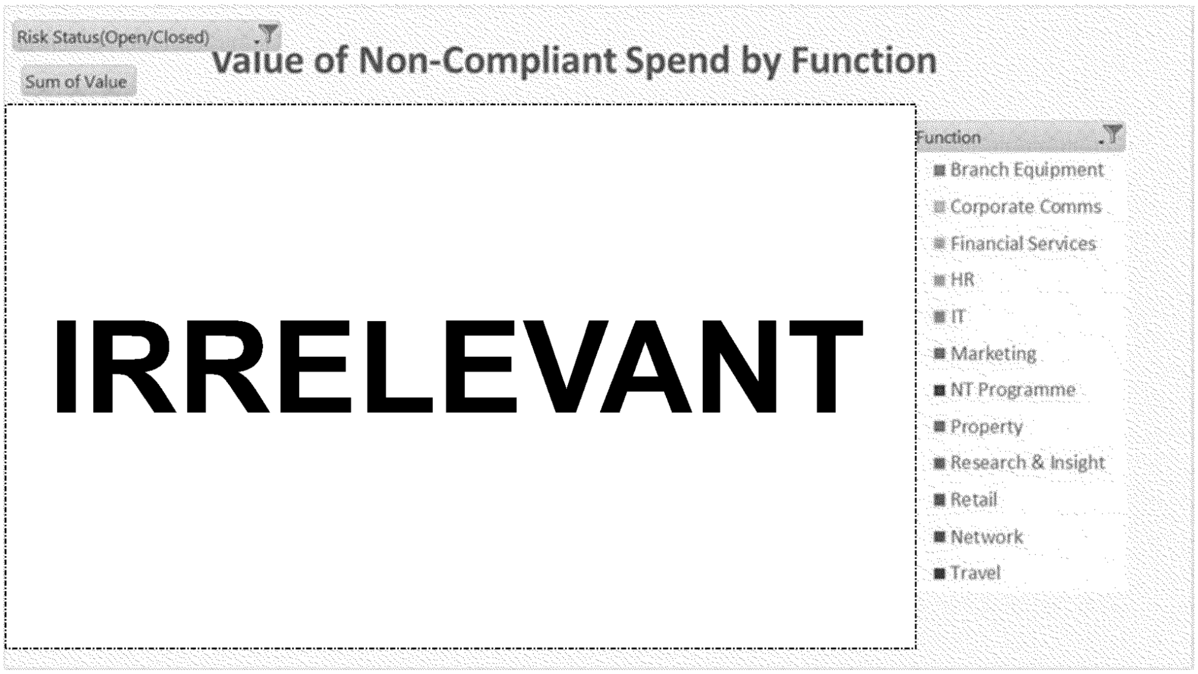
1. *How many and what types of procurement non-compliance have occurred in the past quarter?*
   Since the last RCC report in March there have been a total of 15 non-compliant incidents with a total value of **IRRELEVANT** With the exception of 2 software related items all material [>£164k] items were included in the pipeline of pending non-compliance supplied to the RCC in March.

2. *What are we doing about it?*

   In the past quarter, while we have added IRRELEVANT of new non-compliant spend we have also resolved IRRELEVANT within the quarter, with only a short term contract extension required and some longer term risk positions resolved notably for IRRELEVANT We have reviewed and adjusted forecast spend data against actuals resulting in a small increase in risk exposure overall. Our overall value has therefore risen from IRRELEVANT n July.

Open non-compliant awards since January 2017 are outlined below:

Function	**March - Sum of Value**	**July - Sum of Value**
Branch Equipment	IRRELEVANT	
Corporate Comms		
Financial Services		
HR		
IT		
Marketing		
NT Programme		
Property		
Research & Insight		
Retail		
Network		
Travel		
Grand Total		



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

4. *Why are these incidents occurring, and what can be done about it?*

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

a) Low value, time constrained or highly sensitive/specialist engagements are common. For example, the Board have requested a number of expedited reviews since the New Year on a short turn-around time.
b) Large commercial arrangements cannot often be easily competed or unravelled without operational impact, and re-procurement may be subject to a pending evolution of a supporting Business Strategy.
c) The contractual arrangements may pre-date PCR 2015 regulations or the contract novated during separation from RMG, automatically becoming non-compliant at the renewal point. Non-compliant awards are frequently made on a tactical basis to extend contractual services while public tender processes are executed.

d) Delays to public sector panels of suppliers becoming available. The Post office makes extensive use of this low cost route to market and new/refreshed panels are subject to frequent delays from Crown Commercial Services. Single interim extensions [of periods under 12 months] while tender processes are run are considered to be low risk legally.

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

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

5. *Why are we receiving this report?*

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

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

A full list is appended at Appendix B. Since the last RCC in March 2018, two items have been added, only one of which is material and has been the subject of a paper to GE. The first, for branch design activity has been competitively procured under threshold but is expected to breach threshold over the term. The second is for a one year non-compliant extension to our Payments provider to complete a technology upgrade programme. Tender preparation for the new contract term is already underway.

Conclusion

Non-compliant awards of contracts are already subject to extensive internal governance, legal and risk review, explicit GE and Board approval where value/risks reach a minimum threshold.

The YTD non-compliance value is **IRRELEVANT** *the majority of which are interim extensions while procurement processes are run and to allow for operational migration risk to be mitigated. Individually, all large value non-compliant contracts have been* *reviewed by appropriate Post Office governance forums with agreement on next steps and actions towards remediation allocated where appropriate.*

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

Input Sought

Review and note content only.

The Appendix

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

A full explanation of the individual compliance breaches for direct awards over £181k [previously £164k] threshold is attached in Appendix A. Each entry details the nature of, and the value of the breach.

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

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

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

All contracts entered into during this period were compliant with internal governance processes on contract and commercial review. All were for awards of between £0 and £4,000,000.

3. *Why were the approvals given?*

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

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

There were no unapproved, material breaches during this period.

5. Describe the causes of non-compliance to PCR regulations

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

a) Low value, time constrained or highly sensitive/specialist engagements are common. For example, the Board have requested a number of expedited reviews since the New Year on a short turn-around time.
b) Large commercial arrangements cannot often be easily competed or unravelled without operational impact, and re-procurement may be subject to a pending evolution of a supporting Business Strategy.

c) The contractual arrangements may pre-date PCR 2015 regulations or the contract novated during separation from RMG, automatically becoming non-compliant at the renewal point. Non-compliant awards are frequently made on a tactical basis to extend contractual services while public tender processes are executed.

d) Delays to public sector panels of suppliers becoming available. The Post office makes extensive use of this low cost route to market and new/refreshed panels are subject to frequent delays from Crown Commercial Services.

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

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

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

a) A forward view of material contracts falling under each Business Unit is currently prepared by the relevant Procurement Manager for discussions with their key stakeholders. The maturity of this look ahead view does vary currently and is a high priority activity within the team.

b) Sourcing options papers are prepared for review by contract managers and key stakeholders [risk, legal, security] with routes to market agreed. In many cases these are dependent on evolving business and operating model strategies and the Procurement team are now actively involved with some units helping to advise as thinking evolves.

c) Where a non-compliant award is proposed due to time pressure, Procurement are actively working on long term mitigation with awards made on an interim basis to meet urgent operational needs.

d) Each RCC member will now receive a regular report on compliance within their business unit[s].

e) A new Risk & Governance process requires a Risk Exception report to be created for non-compliant direct awards with SLT or GE sign off.

f) All Professional Services engagements must be approved in writing in advance by the COO. A compliant panel of preferred consulting partners has been appointed and proposed engagements outside of this panel are subject to additional review and challenge.

g) Procurement will now provide training as part of the revised Induction process for new staff. Training packs are being updated for existing staff and made available on the Intranet and ad hoc training sessions for interested Business Units are being run.

h) A new Intranet site has been launched for Procurement to improve visibility of process, regulation, and the panels of approved compliant suppliers available to POL business units.

i) A revised POL Procurement Policy is being drafted giving more granular guidance.
j) Using Crown Commercial Services frameworks, panels of Preferred Suppliers are being refreshed and updated across a wide range of spend categories to reduce time to market, improve compliance and greatly improve commercial outcomes and legal risk.
k) A planned change to operational systems will, once live, give Procurement earlier visibility of potential compliance issues eg: contractual value thresholds.

POL00401627

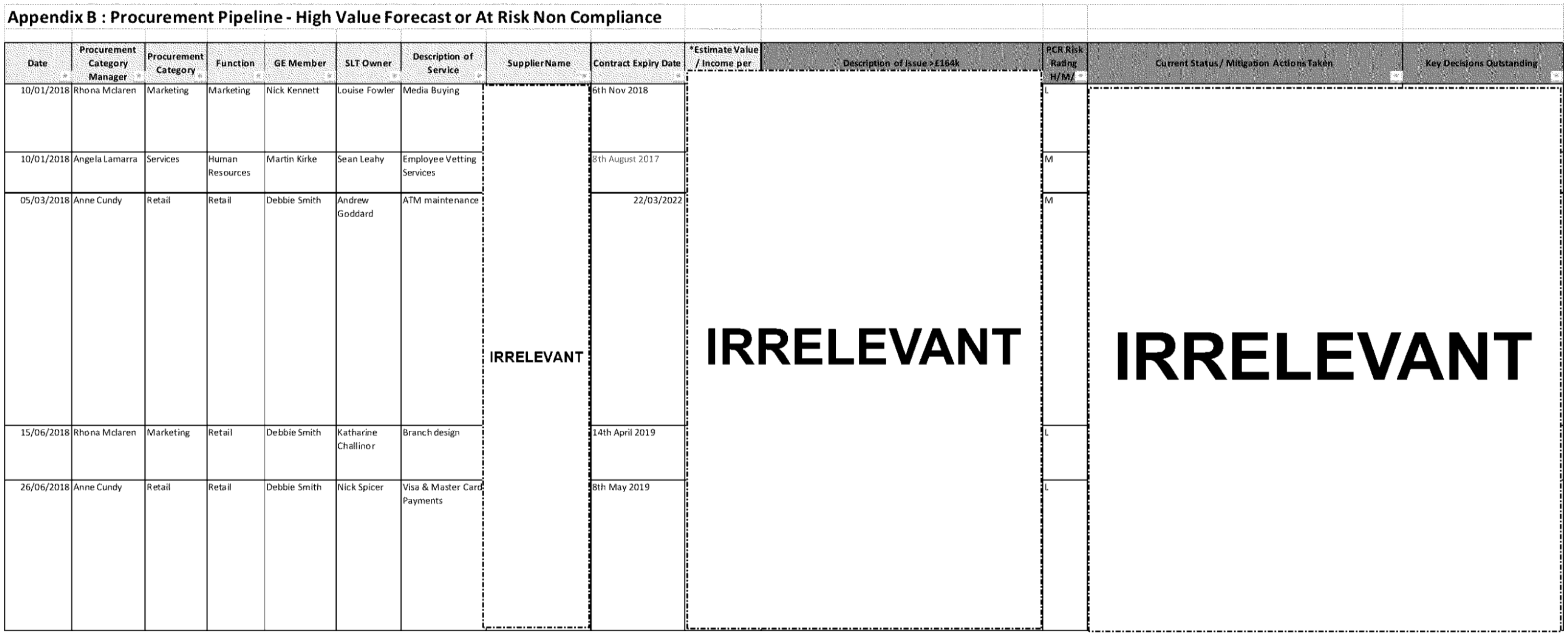
APPENDIX A : RISK LOG - OPEN ITEMS OVER > £164K

Incident Ref No	Date	Category Manager	Procurement Category	Function	GE Member	Value/ Income	Supplier Name	Breach Type 1 - PCR Threshold	Event (what happened) ONLY FOR £25K>	Actions Taken ONLY FOR £25K>	Further Planned Actions ONLY FOR £25K>
	15.02.2017	Angela Lamarra	Comms, R&I & PR	Corporate Comms	Mark Davies	IRRELEVANT		PCR - >£164.5k	IRRELEVANT		IRRELEVANT
2017/0009	21 March 2017	Nicola Sams	Comms, R&I & PR	Research & Insight	Paula Vennells			PCR - >£164.5k		IRRELEVANT	
2017/0013	23 March 2017	Angela Lamarra	Professional Services	HR	Martin Kirke			PCR - >£164.5k			
2017/0019	01 June 2017	Antony Ray	Professional Services	HR	Martin Kirke			PCR - >£164.5k			
2017/0036	30th October 2017	Antony Ray	Professional Services	Financial Services	Owen Woodley			PCR - >£164.5k	IRRELEVANT		
2017/0038	01 January 2018	William Porter	Property	Property	Alisdair Cameron			PCR - >£164.5k			

APPENDIX A : RISK LOG - OPEN ITEMS OVER > £164K											
Incident Ref No	Date	Category Manager	Procurement Category	Function	GE Member	Value/ Income	Supplier Name	Breach Type 1 - PCR Threshold	Event (what happened) ONLY FOR £25K>	Actions Taken ONLY FOR £25K>	Further Planned Actions ONLY FOR £25K>
2017/0041	10 January 2018	Angela Lamarra	Travel	Travel	Alisdair Cameron	IRRELEVANT		PCR - >£164.5k	IRRELEVANT		
2017/0042	10 January 2018	Angela Lamarra	Professional Services	HR	Martin Kirke			PCR - >£164.5k			
2017/0044	10th January 2018	Shahab Hasan	IT Software	IT	Rob Houghton			PCR - >£164.5k			
2017/0048	23 April 2018	Angela Lamarra	Comms, R&I & PR	Corporate Comms	Mark Davies			PCR - >£164.5k			
2017/0049	23 April 2018	Antony Ray	Comms, R&I & PR	Corporate Comms	Mark Davies			PCR - >£164.5k			
2017/0050	23rd April 2018	Rhona Mclaren	Marketing	Marketing	Owen Woodley			PCR - >£164.5k			
2017/0051	23rd April 2018	Rhona Mclaren	Marketing	Marketing	Owen Woodley			PCR - >£164.5k			

APPENDIX A : RISK LOG - OPEN ITEMS OVER > £164K

Incident Ref No	Date	Category Manager	Procurement Category	Function	GE Member	Value/ Income	Supplier Name	Breach Type 1 - PCR Threshold	Event (what happened) ONLY FOR £25K>	Actions Taken ONLY FOR £25K>	Further Planned Actions ONLY FOR £25K>
2017/0052	23rd April 2018	Rhona Mclaren	Marketing	Marketing	Owen Woodley	IRRELEVANT		PCR - >£164.5k	IRRELEVANT		
2017/0057	04 July 2018	Kelly Snares	IT Software	Marketing	Owen Woodley			PCR - >£164.5k			
2017/0059	04 July 2018	Kelly Snares	IT Software	Marketing	Owen Woodley			PCR - >£164.5k			
2017/0057	08 May 2018	Anne Cundy		Retail	Debbie Smith			PCR - >£164.5k			



Appendix B : Procurement Pipeline - High Value Forecast or At Risk Non Compliance

Date	Procurement Category Manager	Procurement Category	Function	GE Member	SLT Owner	Description of Service	Supplier Name	Contract Expiry Date	*Estimate Value / Income per	Description of Issue >£164k	PCR Risk Rating H/M/	Current Status / Mitigation Actions Taken	Key Decisions Outstanding
10/01/2018	Rhona Mclaren	Marketing	Marketing	Nick Kennett	Louise Fowler	Media Buying	IRRELEVANT	6th Nov 2018	IRRELEVANT		L	IRRELEVANT	
10/01/2018	Angela Lamarra	Services	Human Resources	Martin Kirke	Sean Leahy	Employee Vetting Services		8th August 2017			M		
05/03/2018	Anne Cundy	Retail	Retail	Debbie Smith	Andrew Goddard	ATM maintenance		22/03/2022			M		
15/06/2018	Rhona Mclaren	Marketing	Retail	Debbie Smith	Katharine Challinor	Branch design		14th April 2019			L		
26/06/2018	Anne Cundy	Retail	Retail	Debbie Smith	Nick Spicer	Visa & Master Card Payments		8th May 2019			L		

POST OFFICE PAGE 1 OF 3
RISK AND COMPLIANCE COMMITTEE

PCI Compliance Status Update.

Authors: David Meldrum/Ehtsham Ali Sponsor: Rob Houghton Meeting date: 10 July 2018

Executive Summary

Context

As reported at the last meeting, Post Office (PO) have not yet achieved a Report on Compliance (RoC) from our external qualified security assessor (QSA) proving our compliance to the Payment Card Industry-Data Security Standard (PCI-DSS). Although there has been solid progress, PO still have a significant amount of work to do. The existing RoC expired on 28th December 2017 and we have continued to share our remediation plans with Global Payments (GP), our acquirer, who has indicated general support for our plans and have chosen not to implement any challenges to date. We continue to work with the QSA, and our stakeholders, to initiate a more committed and robust regime of compliance.

Questions this paper addresses

1. Why PCI-DSS is important to the PO business?
2. What challenges are faced with the current audit and the risks associated with delay/failure to receive a RoC?
3. What actions are PO taking?
4. Longer term options as the impacts increase?

Conclusion

- PCI-DSS certification is IRRELEVANT PO's ability to evidence continuous work to support PCI-DSS accreditation is essential.
- We have a number of QSA audit non-compliances, and a failure to remediate these could result in some sanctions from our Clients and Partners.
- We have identified 155 remediation activities (96 complete to date) that are being tracked to complete by October 2018. Current dialogue with the QSA, Partners and Clients indicate the risk of sanctions, in the near term, is limited.
- We are initiating an investment in a strategic PCI-DSS solution to resolve the ever increasing challenge of PCI-DSS.

Input Sought

RCC is requested to note this paper and in particularly acknowledge support for a more strategic approach to PCI-DSS compliance subject to PO adequately scoping such work with the QSA and GP accepting this to run alongside the continuous completion of audit actions.

Report

Why PCI-DSS is important to the PO business?

1. PCI-DSS applies to companies of any size that accept or process any card payments data. PO need to host card data securely with the goal of protecting our customer's data.

2. There is a requirement IRRELEVANT IRRELEVANT This is particularly relevant to the Banking Framework.

3. We have a IRRELEVANT in the Banking Framework. We are in the process of undertaking an external audit of the Banking Framework, the scope is with the banks for review, so we expect it to become clear we are not fully PCI-DSS compliant.

Challenges faced with the current audit and the risks associated with delay/failure to receive a RoC?

4. Recent QSA audits in the early part of 2018 indicated that there were a total of 155 PCI-DSS remediation activities required across the estates managed by ComputaCenter and Fujitsu.

5. The Banks IRRELEVANT IRRELEVANT

6. Although we do not have visibility of any potential charges that GP may levy against us for PCI-DSS non-compliance, we have been informed by our QSA that there are a number of formal steps before fines could be levied.

7. Current dialogue with our acquiring bank is positive and we do not yet feel any intention from GP to notify us of their intention to begin the process to levy fines. Providing it is clearly demonstrated that PO is managing the security of the PCI environment and has a commitment to resolving the PCI compliance issues while working closely with an external PCI QSA, then the bank will generally be comfortable and will not issue any fines.

What actions are PO taking?

8. In order to expedite the completion of all identified non-compliances and the remediation of the outstanding control items; PO are doing the following:

    a. Established daily and weekly progress meetings with Computacenter and Fujitsu respectively, working with them in addressing the gaps identified.

    b. Working with both partners to ensure they design and implement the controls or compensating controls to ensure compliance. Providing rigour and challenge to timescales being presented.

9. There are a number of CR's which are being challenged by our supplier Computacenter and several legal letters have been exchanged on who is liable for cost of PCI – DSS compliance.

10. Re-established a PCI Steering Committee with a focused attendee list and senior business representation to drive forward the strategic solutions and keep the business abreast of the progress made.

11. The proposed technical solutions will need to be applied across our entire estate before the QSA can start their assessment and accordingly the Steering Group has agreed with QSA's recommendation to recommence the audit post completion of the remedial actions.

12. Our QSA has confirmed that our environment is locked down and has no Data or IT security exposures. The branch terminals are running on a dedicated isolated network within Post Office branches. All data, including payment card data is sent from the branch terminals to the Fujitsu data centre over a dedicated network connection and protected with strong encryption.

Longer term options as the impacts increase?

13. The PO PCI-DSS estate is increasing over time (Customer Hub and Panther), although these will be covered by separate certifications, not linked with our current PCI-DSS audit.

14. Customer Hub has successfully been launched and we have successfully attained PCI Certification.

15. A robust strategic approach needs to be in place to align us with the other industry retailers, where PO do not store, process or transmit card data.

16. This approach will require investment and time to implement. Nicholas Spicer and his team within Payment Services are compiling a business case for a possible solution.

17. We will establish a dedicated programme of work to progress the longer term strategic solution that reduces our exposure on relying on our suppliers to maintain our PCI-DSS certification.

POST OFFICE
RISK AND COMPLIANCE COMMITTEE

PCI-DSS Compliance Status Report.

Authors: David Meldrum / Ehtsham Ali Sponsor: Rob Houghton Meeting date: 10 July 2018

Executive Summary

Context

As reported at the last meeting, Post Office (PO) are without a Report on Compliance (RoC) from external qualified security assessors (QSA) proving our compliance to the Payment Card Industry-Data Security Standard (PCI-DSS). There has been progress, however PO still do not have a confirmed date when we will be in receipt of our RoC.

The existing RoC expired on 28th December 2017. We have continued to share our remediation plans with Global Payments (GP) our acquirer. Whilst GP could levy penalties against PO, to date, they have not chosen to take this action and there would be extensive dialogue to indicate their intention.

Questions this paper addresses

- Why PCI-DSS is important to the PO business?
- Challenges faced with the current audit and the risks associated with delay/failure to receive a RoC?
- What actions are PO taking?
- Longer term options as the impacts increase?

Conclusion

1. PCI-DSS certification is important to PO as it is a requirement in contracts with Clients and Partners. This has wide reaching impact not only for taking card payments in branch but also for the Banking Framework business.

2. There is no evidence that we would not be able to take card payments and trade without the certification. However, this could impact our ability to meet the North Star strategy to deliver IRRELEVANT profit (grow our business and maximise profits) as winning new business may require PCI-DSS certification as a pre-requisite and our IRRELEVANT IRRELEVANT

3. We have established that remediation activities are being tracked to be completed by October 2018. Of our suppliers who are expected to aid PO in gaining compliance, there are daily progress meetings with Computacenter and twice a week with Fujitsu to ensure they remain on track with the BAU remediation actions.

4. We have set up a programme of work to deliver the strategic solution for PCI-DSS going forwards. This would seek to exclude PO from handling, processing or transmitting card data, and will reduce our dependency on our suppliers to achieve PCI-DSS compliance.

Input Sought

RCC is requested to note this paper.

Report

Why PCI-DSS is important to the PO business?

5. PCI-DSS applies to companies of any size that accept or process any card payments data. PO need to host card data securely with the goal of protecting our customer's data.

6. There is a requirement IRRELEVANT IRRELEVANT This is particularly relevant to the Banking Framework.

Challenges faced with the current audit and the risks associated with delay/failure to receive a RoC?

7. We have a IRRELEVANT in the Banking Framework. Banks are IRRELEVANT IRRELEVANT

8. We in the process of undertaking an external audit of the Banking Framework, the scope is with the banks for review, so we expect it to become clear we are not fully PCI-DSS compliant.

9. The Banks IRRELEVANT IRRELEVANT

10. Although we do not have visibility of any potential charges that GP may levy against us for PCI-DSS non-compliance, we have had to pay higher transactions fees in the past when PO were unable to take contactless payments. In this instance Mastercard Integrity fines, which was IRRELEVANT (minimum charge of IRRELEVANT of the face value of every MasterCard transaction. That equated to IRRELEVANT p.a. but if it included Visa it would have been over IRRELEVANT p.a. in higher charges. We have been informed by our QSA that there are a number of steps before fines are issued, with prolonged dialogue with our acquiring bank whereby they notify us of their intention. Each bank has a different approach depending on their risk appetite. Providing it is clearly demonstrated that the organisation is managing the security of the PCI environment and has a commitment to resolving the PCI compliance issues while working closely with an external PCI QSA, then the bank will generally be comfortable. Prior to issuing fines the bank will generally warn the organisation and issue a deadline date for meeting compliance which if not met, may result in fines. To date GP have not made any mention of additional charges or fines due to non-compliance with PCI.

11. There are a number CR's which are being challenged by our supplier (Computacenter) and several legal letters have been exchanged on who is liable for cost, the proposed technical solution will need to be applied across our entire network before the QSA can start their assessment.

12. To put the issues identified by the QSA into context, we believe that our environment is very locked down and has no Data or IT security exposures. The branch terminals are running on a dedicated isolated network within Post Office

branches. All data, including payment card data is sent from the branch terminals to the Fujitsu data centre over a dedicated network connection and protected with strong encryption. The issues noted are relate to compliance to PCI standards.

What actions are PO taking?

13. In order to expedite the completion of all identified non-compliances and the remediation of the 4 outstanding issues, PO are doing the following:

    a. Established daily progress meetings Computacenter, working with them in addressing the gaps identified.

    b. We have appointed a full time project manager to ensure all issues are addressed in a timely fashion.

    c. PO have been working with CC to ensure they design and implement the controls or compensating controls ensure compliance. Providing rigour and challenge to timescales being presented.

14. -Re-established a PCI Steer-Co with a focused attendee list and senior business representation to drive forward the strategic solutions and keep the business abreast of the progress made.

15. -Clarified the position regarding PODG being in scope of our assessment with our suppliers and QSA, agreed that this will be proposed to be de-scoped from the PCI audit through discussions with our acquiring bank which our QSA will support.

Longer term options as the impacts increase?

16. The PO PCI-DSS estate is increasing over time (Customer Hub and Panther), although these will be covered by separate certifications, not linked with our current PCI-DSS audit. Customer Hub has successfully been launched and they have attained their own PCI Certification.

17. A robust strategic approach needs to be in place to align us with the other industry retailers, where PO do not store, process of transmit card data. This approach will require investment and time to implement. Nicholas Spicer and his team within Payment Services are compiling a business case for a possible solution.

18. Established a dedicated programme of work to progress the longer term strategic solution that reduces our exposure on relying on our suppliers to maintain our PCI-DSS certification.

Gifts & Hospitality Annual Review 2017-18

Author: Sally Smith Sponsor: Jane MacLeod Meeting Date: July 2018

Executive Summary

Context

As part of our annual Anti-Bribery and Anti-Corruption (ABC) obligations, this paper provides an overview of the Gifts & Hospitality reporting for the period 2017-18.

Questions addressed in this paper

- What issues have been highlighted based upon the review?
- What actions need to be undertaken to address any issues?

Conclusion

1. Whilst there have been breaches relating to adherence to the policy, we have not identified any instances indicative of Bribery or Corruption.

2. Quality and quantity of gifts and hospitality reporting has greatly improved compared to the same period last year, although there is still more that needs to be done to change the culture in relation to the correct reporting and approval.

Input Sought

The R&CC is asked to review this report and consider whether any further actions should be taken to further improve gifts and hospitality reporting.

The Report

Summary of ABC activities relating to Gifts & Hospitality reporting 2017-18

1. The new reporting tool was delivered in August 2017, and an FAQ area has been added to the reporting tool covering common questions and reporting issues
2. Quarterly reporting to all GE members commenced from October 2018, summarising overall Post Office reporting and highlighting any breaches or concerns for each GE's business area.
3. There have been 3 communications issued relating specifically to Gifts and Hospitality reporting.
4. Enhanced mandatory ABC training was delivered in September 2017 and this is now tracked from weekly Success Factors reports by HR Directors.

Summary of Gifts & Hospitality received and offered 2017-18

5. Analysis of the 2017-18 Gifts & Hospitality Register has highlighted that the quality of submissions made in this period compared to the same period last year has greatly improved (please see Appendix A & B for data):
   - In 2016/17 there were 17 gift reports totalling £230 and 128 hospitality reports totalling £5475.55
   - In 2017/18 there were 27 gift reports totalling £1521 and 195 hospitality reports totalling £33,673.07
6. Whilst an improvement has been seen, it is believed that there is still significant under-reporting, particularly relating to gifts and declined offers.
7. In the reporting period, the following common breaches were identified:
   - A number of instances where employees have accepted gifts of cash or cash equivalent (e.g. gift cards). Whilst the members of staff reported these, cash gifts are against policy and should have been returned to the customer. These instances were reported to relevant line managers after the report was submitted to ensure that the gifts were returned and further guidance given to staff members.
   - There have been a number of instances where offers of hospitality have been submitted and approved retrospectively. Again, guidance has been given to relevant line managers and individuals.
   - A trend has been identified where submissions are being reported with the title description "Hospitality" rather than, for example, "dinner with x". The title field of the reporting tool has been amended to assist users to correctly report submissions.
8. A review of the external companies that have offered hospitality to Post Office in 2017/18 has not identified any significant issues, and the top 6 are detailed below:

External Party Name	**Volume**	**People**	**Value**
FRES (First Rate Exchange Services)	22	24	£ 2,580.00
Kings Security	6	6	£ 1,780.00
CMS LLP	8	31	£ 1,200.00
Womble Bond Dickinson	6	22	£ 1,130.00
Chemistry Club	7	16	£ 540.00
Bank of Ireland	6	7	£ 369.22

Planned actions to address issues:

9. The following activities are planned to improve the quality and effectiveness of gifts and hospitality reporting and approval:
    - ABC training is scheduled for the end of July 2018 and the content has been amended to help address common failings identified during 2017-18 and make the reporting and approval requirements easier to understand
    - A summer reminder communication is scheduled to be issued during July, with further communication and awareness activity planned throughout the year
    - Financial Crime will continue to monitor gifts and hospitality reporting and feedback to individuals and line management

Appendix A – Gifts and Hospitality for 2017/18

The below tables sets out all gifts and hospitality offered and received by GE member:

Pre-Introduction of the Gifts and Hospitality Reporting Tool:

1st April 2017- 7th August 2017	**Gift**		**Hospitality**		**Total**	
Business Team	**Volume**	**Value**	**Volume**	**Value**	**Volume**	**Value**
Communication, Brand & Corporate Affairs	0	£0.00	0	£0.00	0	£0.00
Finance and Operations	0	£0.00	4	£320.00	4	£320.00
Financial Services and Telecoms	0	£0.00	13	£2,348.00	13	£2,348.00
HR	1	£0.00	0	£0.00	1	£0.00
IT	1	£60.00	1	£400.00	2	£460.00
Legal, Risk and Governance	0	£0.00	12	£2,827.00	12	£2,827.00
Retail	0	£0.00	8	£1,010.00	8	£1,010.00
Strategy	0	£0.00	0	£0.00	0	£0.00
Grand Totals	**2**	**£60.00**	**38**	**£6,905.00**	**40**	**£6,965.00**

Post Introduction of the Gifts and Hospitality Reporting Tool:

8th August 17- 31st March 18	**Gift**		**Hospitality**		**Total**	
Business Team	**Volume**	**Value**	**Volume**	**Value**	**Volume**	**Value**
Communication, Brand & Corporate Affairs	1	£35.00	5	£1,534.00	6	£1,569.00
Finance and Operations	8	£511.00	19	£5,662.00	27	£6,173.00
Financial Services and Telecoms	6	£180.00	46	£5,223.07	52	£5,403.07
HR	0	£0.00	8	£625.00	8	£625.00
IT	0	£0.00	5	£399.00	5	£399.00
Legal, Risk and Governance	3	£130.00	56	£11,338.00	59	£11,468.00
Retail	7	£605.00	17	£1,887.00	24	£2,492.00
Strategy	0	£0.00	1	£100.00	1	£100.00
Grand Totals	**25**	**£ 1,461**	**157**	**£ 26,768.07**	**182**	**£ 28,229.07**

Appendix B – Gifts and Hospitality for 2016/17

The below tables sets out all gifts and hospitality reported for the 2016/17 financial year:

Gifts		**Hospitality**	
Total volume	17	*Total volume*	128
Total value	£230.00	*Total value*	£5,475.55
Amount without value recorded	7	*Amount without value recorded*	100
Amount with value recorded	10	*Amount with value recorded*	28
Declined	1	*Declined*	14
Value within policy amount (<£200)	10	*Value within policy amount (<£100)*	23
Value above policy amount (>£200)	0	*Value above recommended policy amount (>£100)*	5 (all authorised in line with Policy)
Policy Breaches	1 – acceptance of £100 cash	*Policy breaches*	0

As reported last year, due to the inconsistencies in the information captured data could not be properly analysed and due to structural changes within Post Office during the 2016/17 financial year it is not possible to compare the separate business areas.

Anti-Bribery & Anti-Corruption Policy

Author: Sally Smith Sponsor: Jane MacLeod Meeting Date: 10th July 2018

Executive Summary

Context

This paper sets out the updates and revisions to the Anti-Bribery and Anti-Corruption (ABC) Policy as part of the annual review process for the Risk and Compliance Committee to consider and approve.

Questions addressed in this paper

- What changes to the Policy do we propose and why?
- What are the implications of these changes?

Conclusion

1. The ABC Policy has been amended to ensure it reflects industry best practice and provide clarity as to role and responsibilities in relation to the minimum control standards.
2. The updated Policy reflects queries and issues received by the Financial Crime team over the last 12 months.

Input Sought

The R&CC is asked to approve the updated ABC Policy.

The Report

Why do we need to review this Policy?

3. The Policy was last reviewed and approved by the R&CC in July 2017. The terms of the Policy require it be reviewed annually.

What changes to the Policy do we propose and why?

What are the key features that we propose and why?

4. There have been no legislation changes in the past year and no significant amends made to the policy at this annual review.
5. Minor amends have been made in relation to:
   - The location on the Intranet of the Risk Exception process
   - Mandatory ABC training for all staff has been included in the minimum control standards as a key preventative control
   - Gifts and hospitality minimum control standards have been amended to clarify line management and Financial Crime responsibilities in approving, reviewing and monitoring submissions
   - To reflect industry best practice, charity donations risk area has been amended to include sponsorship, with a new control that the relevant GE member approves any cash donations or sponsorship made by Post Office

How did we develop these recommendations?

6. A review of bribery and corruption cases and penalties publicly reported over the last 12 months and cases that the Financial Crime team has been involved in via the Joint Money Laundering Intelligence Taskforce.
7. Policy queries and issues that have arisen over the previous 12 months have been reviewed to ensure that these concerns are addressed. The definitions have been updated to clarify queries and issues raised by key stakeholders.

What are the implications of these changes?

What will we need to do and by when, to implement and embed these Policy changes?

8. No material changes are required to comply with this updated Policy.
9. All employees need to ensure that they accurately report all instances of gifts and hospitality offered and declined using the reporting tool to obtain appropriate approval.
10. Internal communications and training – once the Policy has been approved, there will be a One communication to advise all employees with a link to the updated document and the Gifts and Hospitality Tool on the Post Office Intranet.
11. The Financial Crime Team will continue to provide quarterly reports to Group Executive members.
12. Every six months, as part of the Group Executive declaration the members are required to confirm that the Policy has been correctly applied in their business area.

What will the impact be on our wider business?

13.Increased transparency of the ABC framework and commitment to maintaining visible compliance with the applicable legislation.

14.Reinforcement that the failure to comply with the requirements of ABC Policy by any employee will be regarded as a significant breach impacting on the Post Office's risk and control management environment and may lead to disciplinary action up to and including dismissal and possible prosecution.

15.The Financial Crime Team monitor adherence to the minimum control standards set out in the Policy on an on-going basis through their review of the Gifts and Hospitality Tool and any other reported issues - any control gaps identified are reported to the R&CC as required. Appendix A provides an overview of the assurance checks developed by the Financial Crime team during 2017/18.

What would the impact be of delaying approval?

16.Risk that the group breaches the Bribery Act 2010 by not having up to date policies and procedures to prevent bribery by any person or company who operates on our behalf.

17.Post Office Limited is required to maintain up to date policies to support contractual requirements with clients and suppliers (e.g. MoneyGram and the Partner Banking Framework) and failure to do so may result in a breach of contract, and whilst not material, could have commercial and reputational impacts.

18.Post Office Limited provides Post Office Management Services (POMS) with its policies suite in the form of "Group Policies". POMS is required under its regulatory responsibility to the Financial Conduct Authority to have up to date policies and failure to do so may lead to regulatory sanctions or penalties.

Appendix A - ABC Policy Minimum Control Standards Assurance

The below table shows the residual risk rating from a first and second line of defence perspective for each control type within the currently approved policy as at the Q1 2018/19 review

Risk Description	Control Type	Description of control	Residual risk rating			Control Strength		Q1 Assurance Comments
			L	I	S	1st LoD	2nd LoD	
Failure to ensure that Consultants and Contractors comply with the Group's anti-bribery and corruption policy	Preventative	(a) Training of contractors; (b) Contractual compliance with policies by consultants.	3	3	9	Partially effective	Effective	Weekly report from SF provided to all HR directors for them to follow through with individuals who have not completed mandatory training as required. During checks undertaken by FC in April it was noted that the percentage of completion by contractors was down to 88% and a chaser was sent to the HR Director. Latest completion rates showing improvement to 92%. Weekly monitoring in place. Not all contracts currently include ABC requirements. 1LOD assessed as partially effective as drop in training completion observed during quarter and some contract gaps.
Insufficient controls may lead to the donation of money to an unregistered charity, which could be interpreted as bribery	Preventative	(a) Validate charity via The Charity Commission. (b) Training of all employees	2	2	4	Effective	Partially effective	No mention of the protocol associated with charities in G&H reporting. ABC policy refers to charity donations, and guides user to a web link which opens a page with error and is being fixed. The G&H process doc is currently being updated and ABC training enhanced.
Insufficient controls may lead to the donation of money to an unregistered charity, which could be interpreted as bribery	Detective	(a) Monitoring of Training attempts	2	2	4	Effective	Partially effective	No mention of the protocol associated with charities in G&H reporting. ABC policy refers to charity donations, and guides user to a web link which opens a page with error and is being fixed. The G&H process doc is currently being updated and ABC training enhanced.
The acceptance of hospitality or gifts from third parties could lead to bias or undue influence, or the perception of such, in how individuals	Preventative	(a) G&H approval process (b) ABC Training	2	3	6	Partially effective	Effective	Report sent to all GE in April and summary included in May RCC report. Specific failures called out in May report and FC continue to monitor inbox for non-conformances. Annual training brought forward to July will highlight weaknesses identified throughout year.

Risk Description	Control Type	Description of control	Residual risk rating			Control Strength		Q1 Assurance Comments
			L	I	S	1st LoD	2nd LoD	
exercise their duties and responsibilities.								
Failure to identify employees requesting or receiving something of value from a third party in exchange for providing employment or work opportunities may result in the loss of Group stakeholder support.	Preventative	(a) Review of all employment	2	3	6	Effective	Effective	Employment process is robust. All employees subject to on boarding policy and procedures and employee data held in success factors
Inadequate controls may lead to employees accepting gifts that are not appropriate, proportionate or within policy resulting in reputational damage or criminal prosecution.	Preventative	(a) G&H reporting tool with clear process in place to be completed when a colleague receives or offers a gift over the value of £20; (b) LM and GE approval required where appropriate; (c) Prohibit accepting cash or equivalents; (d) Group wide training programme	2	3	6	Partially effective	Effective	Report sent to all GE in April and summary included in May RCC report. Specific failures called out in May report and FC continue to monitor inbox for all non-conformances. Annual training brought forward to July will highlight weaknesses identified throughout year.
Inadequate controls may lead to employees accepting gifts that are not appropriate, proportionate or within policy resulting in reputational damage or criminal prosecution.	Corrective	(a) Corrective action when required.	2	3	6	Partially effective	Effective	FC monitor all reports received and instigate corrective action where required. To date, no instances have required escalation to HR.

Risk Description	Control Type	Description of control	Residual risk rating			Control Strength		Q1 Assurance Comments
			L	I	S	1st LoD	2nd LoD	
Inadequate controls may lead to employees accepting hospitality that are not appropriate, proportionate or within policy.	Preventative	(a) G&H reporting tool with clear process in place to be completed when a colleague receives or offers Hospitality; (b) LM and GE approval required where appropriate; (c) Hospitality must be reasonable, ordinarily below the value of £200; (d) Group wide training programme	3	3	9	Partially effective	Effective	Report sent to all GE in April and summary included in May RCC report. Specific failures called out in May report and FC continue to monitor inbox for all non-conformances. Annual training brought forward to July will highlight weaknesses identified throughout year.
Inadequate controls may lead to employees accepting hospitality that are not appropriate, proportionate or within policy.	Corrective	(a) Corrective action when required.	3	3	9	Partially effective	Effective	FC monitor all reports received and instigate corrective action where required. To date, no instances have required escalation to HR.
Offering facilitation payments, gifts & entertainment, client training programmes, charitable or political donations, ex-gratia payments or legal settlements that are not justifiable or proportionate.	Preventative	(a) Conflicts of Interest policy; (b) G&H reporting tool; (c) Group wide training (d) Group Legal Director approval for ex-gratia payments (e) Group wide training programme	1	4	4	Partially effective	Partially effective	CoI policy was due for renewal Mar 2017. Policy referred to CoSec who are undertaking review and update. On Diary for update end June. Existing policy is available on intranet. Assessed as partially effective as policy is currently out of date.
Employees making or soliciting political donations on behalf of Post Office	Preventative	(a) GE approval (b) Prohibit giving Political donations/Gifts	2	2	4	Effective	Partially effective	G&H process doc states that G&H associated with political parties/ representatives is to be avoided. Comms and awareness improvements needed

Risk Description	Control Type	Description of control	Residual risk rating			Control Strength		Q1 Assurance Comments
			L	I	S	1st LoD	2nd LoD	
Inadequate monitoring may lead to third parties engaging in bribery or corruption while performing services on behalf of the Post Office Group.	Preventative	(a) CFO review of fees paid (b) Review of new/ existing contracts; (c) Conflicts of Interest policy	2	2	4	Effective	Partially effective	Psuite has been agreed and signed off and includes specific ABC clauses. Procurement aware of requirements around lock downs. Assessed as partially effective as lock down is reliant on individuals compliance and there are no system controls.

GROUP POLICIES

Anti-Bribery and Corruption Policy

Version – V2.1

Chief Executive's Endorsement

The Post Office Group is committed to doing things correctly. Our Values and Behaviours represent the conduct we expect. This Policy supports these to help us ensure the highest standards of financial crime prevention, detection and management are maintained.

1. Overview

1.1. Introduction by the Policy Owner

The General Counsel has overall accountability to the Board of Directors for the design and implementation of controls to prevent or deter Bribery and Corruption. Anti-Bribery and Corruption is an agenda items for the Audit and Risk Committee and the Post Office board is updated as required.

1.2. Purpose

This Policy has been established to set the minimum operating standards relating to the management of our Bribery and Corruption risks throughout the Group[1]. It is one of a set of policies which provide a clear risk and governance framework and an effective system of internal control for the management of risk across the Group. Compliance with these policies supports the Group in meeting its business objectives and to balance the needs of shareholders, employees[2] and other stakeholders.

1.3. Core Principles

To offer a bribe is a criminal offence; bribery is an offer, promise, payment, request, or agreement to receive anything of value from any person or entity in order to induce that person to perform their roles improperly.

In order to prevent Bribery and Corruption the governance arrangements described in this Policy are based upon the following core principles:

- The Group is committed to and oversees the implementation of a Policy of zero tolerance, recognising that bribery is contrary to fundamental values of integrity, transparency and accountability and undermines the Group's effectiveness;
- Post Office has devised a robust Policy and associated procedures (set out in this document) which are proportionate to the risks and complexity of the Group;
- A bribery risk assessment is an integral part of our Group's overall and ongoing risk management process;
- Post Office must assess the risk associated with entering into joint ventures, partnerships or contracting arrangements with other entities and must carry out periodic due diligence based on that risk assessment. This includes ensuring that these organisations have policies and procedures which are equivalent to the Group's own procedures;
- The Group undertakes a training and awareness program to ensure employees are aware of the potential risks, how bribery might affect them, what they should do if they are offered a bribe, and the consequences should they be found to have made or received a bribe;
- The interests of Policyholders and other stakeholders are protected by ensuring that excessive powers are not delegated to individuals;

[1] In this Policy "Post Office" and "Group" mean Post Office Limted and Post Office Management Services Limited.

[2] In this Policy "employee" means permanent staff, temporary including agency staff, contractors, consultants and anyone else working for or on behalf of Post Office.

- Decisions taken by management are consistent with the Group's strategic objectives and risk appetite, which are approved by the Board;
- Appropriate conduct is demonstrated in executing the requirements contained within the Policy;
- Every member of staff is responsible for understanding and managing the risk they take on behalf of the Group and for ensuring that they act within accordance to them;
- All employees are required to comply with Group Policies.

1.4. Application

This Policy is applicable to all areas within the Group and defines the minimum standards to control financial loss, customer impact, regulatory breaches and reputational damage in line with the Group's Risk Appetite.

In exceptional circumstances, where risk sits outside of the Group's accepted Risk Appetite a Risk Exception can be granted. F~~or f~~urther information in relation to the risk exception process, together with a template can be found on the Intranet..... ~~please contact the Risk & Assurance team – adnan.killedar~~ GRO ~~or georgina.blair~~ GRO

While Post Office does not tolerate events that are criminal in nature and which may give rise to unacceptable and illegal behaviour, it recognises that despite its many endeavours, it is not possible to eliminate all risks of internal and external Bribery and Corruption. As a result Post Office may incur losses, and therefore takes a risk based approach to Bribery and Corruption.

For definitions please see section 3.1.

The risk to the Group in relation to Bribery and Corruption is reviewed by the board on a regular basis.

1.5. Types of Bribery and Corruption Risk

Post Office is exposed to a number of the above risks relating to Bribery or Corruption. These risks include, but are not limited to, the following:

1. **Payment Risks** –for example, facilitation payments, gifts & hospitality, client training programmes, charitable or political donations, ex-gratia payments/ legal settlements. This would also include the offer of sponsorships or grants.
2. **Third Party/Associated Party Risks** –third parties who provide services on behalf of the Post Office Group engaging in bribery or corruption while performing such services. The scope of this could include agency operators within the Post Office network and suppliers procured through the business or through the Procurement Team. Examples of Associated Parties include agents, consultants, suppliers, introducers, and intermediaries.

3. **Employment Risks** –Post Office employees requesting or receiving something of value from a third party in exchange for providing employment or work opportunities at the Post Office or offering or providing work opportunities, paid or unpaid, to Connected Individuals[3], or otherwise using employee connections to improperly obtain business or secure an advantage for Post Office. Employment opportunities (including work experience, secondments, etc.) have a value to the recipient and/or their close family members and may be considered to be bribes if used to improperly obtain or retain business or secure an advantage for Post Office.

4. **Inducement Risks -** Post Office must take reasonable steps to ensure that it, and any person acting on its behalf, does not:
   - Offer, give, solicit or accept an inducement; or
   - Direct or refer any actual or potential business in relation to another person on its own initiative or on the instructions of an associate; if it is likely to conflict to a material extent with any duty that Post Office Management Services owes to its customers in connection with an insurance mediation activity or any duty which such a recipient firm owes to its customers in connection with an insurance mediation activity.

5. **Gifts & Hospitality** –The Group has a process for reporting Gifts & Hospitality (both received and offered) details of this can be found here.

1.6. Legislation

The Group seeks to comply with all relevant UK legal and regulatory requirements including (but not limited to):

- The Bribery Act 2010
- The Criminal Finances Act 2017
- Financial Conduct Authority (FCA) Rules and Guidance (to the extent that these apply – see 1.8 below)

Under the Bribery Act, it is an offence to:

- Directly, or indirectly offer, promise or give a financial or other advantage with the intention of inducing any person to perform a business activity improperly or to reward any person for doing so;
- Request, agree to receive or accept a bribe, i.e. to receive a financial or other advantage with the intention of performing a business activity improperly;
- Bribe a foreign public official;
- Fail to prevent bribery by any person who perform services for or on behalf of a company ("corporate offence").

Post Office is subject to the Bribery Act 2010 (Bribery Act) and could become criminally liable as a result of an act of bribery or corruption by its employees or a third party operating on our behalf.

The Bribery Act has extra-territorial effect which means that the actions of Post Office or a third party operating on our behalf outside of the UK may fall within the scope of the Act. In the context of Post Office, this could apply in scenarios such as where a Post Office contractor or supplier resides outside the UK.

[3] Connected Individuals means those individuals who are known to have close connections to existing or prospective clients or suppliers, Public Officials, Politically Exposed Persons (PEP) or using employees' connections to improperly obtain business or secure an advantage for Post Office.

The Criminal Finances Act also includes a 'failure to prevent' (strict liability) offence on the Group, where failure to prevent criminal facilitation of a tax evasion offence, by a taxpayer, takes place and there are no reasonable procedures put in place to prevent such facilitation, or it cannot show that these procedures would have been unreasonable.

Post Office can be held liable unless it can demonstrate that it has in place "adequate procedures" designed to prevent this type of misconduct. The controls outlined in this Policy, including appendices, assist Post Office in preventing and detecting corrupt conduct and form an essential component of Post Office's adequate procedures.

1.7. FCA Rules

Post Office Limited is an Appointed Representative of the Bank of Ireland and Post Office Management Services Limited (POMS) and is contractually required to comply with certain regulatory requirements. As such the Group as a whole is obliged to ensure there are adequate systems and controls are in place to mitigate Financial Crime risks.

POMS is a directly regulated firm with the FCA is directly exposed to regulatory fines and censure if the FCA determine that the systems and controls associated with this Policy are not effectively implemented.

This Policy contributes to Post Office's compliance with these regulatory and contractual obligations.

2. Risk Appetite and Minimum Control Standards

2.1. Risk Appetite

Risk Appetite is the extent to which the Group will accept that a risk might happen in pursuit of day to day businesses transactions. It therefore defines the boundaries of activity and levels of exposure that the Group are willing and able to tolerate.

The Group takes its legal and regulatory responsibilities seriously and consequently has[4]:

- **Tolerant risk appetite** for Legal and Regulatory risk in those limited circumstances where there are significant conflicting imperatives between conformance and commercial practicality
- **Averse risk appetite** for litigation in relation to high profile cases/issues
- **Averse risk appetite** for ligation in relation to Financial Services matters
- **Averse risk appetite** for not complying with law and regulations or deviation from business' conduct standards for financial crime to occur within any part of the organisation
- **Averse Risk Appetite** in relation to unethical behaviour by our staff.

The Group acknowledges however that in certain scenarios even after extensive controls have been implemented a product or transaction may still sit outside the agreed Risk Appetite. In this situation, a risk exception waiver will be required[5].

2.2. Policy Framework

Post Office has established a suite of financial crime policies and procedures, on a risk sensitive approach which are subject to an annual review. The Policy suite is designed to combat money laundering, terrorist financing, bribery and corruption and adhere to relevant Sanctions regimes. These have been developed to comply with applicable legislation and regulation and covers the following specifically:

- The identification of potential financial crime risks
- On a risk sensitive approach, performing due diligence at on-boarding, periodic basis and payment on third parties who perform services for or on behalf of us.
- Maintaining appropriate records for at least the minimum UK prescribed periods.
- Completing compliance oversight monitoring to test the Group's controls and confirming effectiveness and adherence to financial crime policies.
- Establishing and maintaining Standards for Management Information on Financial Crime. This includes, but is not limited to, record keeping, reporting of suspicious activity and details of staff training.

The Anti-Bribery and Corruption Policy is a key Policy under the Financial Crime Policy framework and should be considered and read in conjunction with the overarching Financial Crime Policy where relevant.

[4] The Risk appetite was agreed by the Groups Board January 2015

[5] For more information in relation to Risk Exception waivers please see section 1.4

2.3. Who Must Comply?

Compliance with this Policy is mandatory for all Post Office employees and applies wherever in the world the Group's business is undertaken. All third parties who do business with the Group, including consultants, suppliers and business and franchise partners, will be required to agree contractually to this Policy with their own equivalent Policy.

Where non-compliance is identified the matter must be referred to the Director of ~~Risk and~~ Compliance and the Group Legal Director. Any investigations will be carried out in accordance with the Investigations Policy. Where is it identified that that an instance of non-compliance is caused through wilful disregard or negligence, this will be treated as a disciplinary offence.

All Post Office employees are required to report any knowledge or suspicions in relation to Bribery or Corruption to Grapevine. As such all business units are required to have a process in place for reporting Bribery or Corruption incidents to Grapevine by telephone on GRO For more information in relation to reporting knowledge or suspicions please see section 3.2.

The next page sets out the minimum control standards that the Group has implemented to control these risks.

2.4. Gifts and Hospitality Tool

The purpose of the Gifts and Hospitality Tool is to make it easy for our employees to accurately record the offering and acceptance of gifts and hospitality throughout the Group. For more information in relation to the tool and how to use this, please see the below links:

The Gifts and Hospitality Tool can be found here.

Instructions upon how to complete the tool can be found here.

The procedure for completing the Gifts and Hospitality Tool can be found here.

2.5. Minimum Control Standards

A minimum control standard is an activity which must be in place in order to manage the risks so they remain within the defined Risk Appetite statements. There must be mechanisms in place within each business unit to demonstrate compliance. The minimum control standards can cover a range of control types, i.e. directive, detective, corrective and preventive which are required to ensure risks are managed to an acceptable level and within the defined Risk Appetite.

The table below sets out the relationships between identified risk and the required minimum control standards in consideration of the stated risk appetite. The subsequent pages define the terms used in greater detail:

Risk Area	**Description of Risk**	**Minimum Control Standards**	**Who is responsible**	**When**
Appointment and Activities of Consultants and Contractors	Failure to ensure that Consultants and Contractors comply with the Group's anti-bribery and corruption policy may lead to criminal prosecution and damage to the Post Office brand or reputation.	Preventative Control: Our contracts require Consultants and Contractors to comply with the Group's anti-bribery and corruption policy. A clause is included within Consultants and Contractors contracts requiring them to comply with the Group's anti-bribery and corruption policy.	Procurement	Ongoing where required
Charity Donations and Sponsorship	Insufficient controls may lead to the donation of money to an unregistered charity, which could be interpreted as bribery and result in reputational damage.	Preventative Control: Where the Group, a team or an individual has selected a particular charity to support, they are required to validate that charity against the Charity Commissions website. More information can be found here. Where a supplier or third party requests that Post Office makes a charitable donation, Post Office ensures that the donation	All employees	Ongoing

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
		is not linked to any business or services provided to or by that supplier or third party. Any cash donations or sponsorship should be approved by the relevant GE member to ensure appropriateness[SS3] Post Office has a Group wide training programme to ensure that all customer facing staff, back office staff and contractors receive adequate training. Staff and contractors are required to complete training within 30 days of joining Post Office and annually[SS4]. Outsource providers, clients & suppliers must maintain records to evidence that staff have received adequate and regular training. Detective Controls: Pass rate and number of test attempts is monitored to identify risk areas and any additional training or guidance required.	All employees GE are responsible for approval of cash donations and sponsorship Human Resources is responsible for any incidents where further action is required and ensuring completion of mandatory training Financial Crime Team is responsible for reviewing training effectiveness	Ongoing
Conflicts of Interest	The acceptance of hospitality or gifts from third	Preventative Control:	All employees	Ongoing

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
	parties could lead to bias or undue influence, or the perception of such, in how individuals exercise their duties and responsibilities.	The Group operates a procedure to ensure Gifts and Hospitality may not be offered or accepted where they could bias or influence how individuals exercise their duties and responsibilities. All employees are made aware of and are expected to comply with the gifts and hospitality procedures.		
Employment Risks	Failure to identify employees requesting or receiving something of value from a third party in exchange for providing employment or work opportunities may result in the loss of Group stakeholder support.	Preventative Control: Any form of employment or work opportunities (paid or unpaid) must be reviewed and approved prior to employment.	All employees	Ongoing
Gifts	Inadequate controls may lead to employees accepting gifts that are not appropriate, proportionate or within policy resulting in reputational damage or criminal prosecution.	Preventative Control: All employees must report correctly ~~any~~ all gifts ~~or hospitality~~ of £20 and over which they receive or offer using the Gifts & Hospitality tool, whether accepted or declined. No employee may accept cash (or cash equivalent) gifts.	Each employee is responsible for ensuring that all gifts offered or received are recorded. Line managers are responsible for ensuring the gift complies with	Ongoing Ongoing Ongoing

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
		Post Office has a Group wide training programme to ensure that all customer facing staff, back office staff and contractors receive adequate training. Staff and contractors are required to complete training within 30 days of joining Post Office and annually. Corrective Control: Where an issue is identified, the reason for this is reviewed and action is taken. Action may include~~s~~ disciplinary and dismissal.	policy and is reasonable and for approving or declining the acceptance of a gift[SS5] Group Executive are~~is~~ responsible for approving or declining any offers over £100 Financial Crime Team is responsible for ~~reviewing~~ reviewing and monitoring the Gifts and Hospitality register. Human Resources is responsible for ~~reviewing~~ any incidents where further action is required and ensuring completion of mandatory training	Ongoing Ongoing
Hospitality	Inadequate controls may lead to employees accepting hospitality that is not appropriate, proportionate or within policy resulting in reputational damage or criminal prosecution.	Preventative Control: All employees must report correctly any ~~gifts or~~ hospitality which they receive or offer using the Gifts & Hospitality tool, whether accepted or declined[SS6]. Before accepting or giving hospitality an employee must receive written approval from their line manager.	Each employee is responsible for ensuring that all hospitality offered/received are recorded Line managers are responsible for ensuring the gift complies with policy and is reasonable and for approving or	Ongoing Ongoing Ongoing

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
		The hospitality must be reasonable (not lavish or extravagant), proportionate to its purpose and must ordinarily be below £200 per person in value. Post Office has a Group wide training programme to ensure that all customer facing staff, back office staff and contractors receive adequate training. Staff and contractors are required to complete training within 30 days of joining Post Office and annually.	declining the acceptance of hospitality Group Executive are~~is~~ responsible for the approving or declining of any offers of hospitality over £200 Financial Crime Team is responsible for reviewing and monitoring the Gifts and Hospitality register Human Resources is responsible for ~~reviewing~~ any incidents where further action is required and ensuring completion of mandatory training	Ongoing Ongoing
Payment Risks	Offering facilitation payments, gifts & entertainment, client training programmes, charitable or political donations, ex-gratia payments or legal settlements that are not justifiable or proportionate may result in reputational damage or criminal prosecution.	Preventative Control: All employees are required to comply with the conflicts of interest policy which can be found here. All employees are required to comply with the Gifts and Hospitality procedure which can be found here. The acceptance of discounted or complimentary training courses which would usually incur a cost are classified as Gifts and	Each employee is responsible for ensuring that all hospitality and gifts offered or received are recorded Line managers are responsible for approving or declining the acceptance of a gift or hospitality. Group Executive are~~is~~ responsible for the approving or declining of	Ongoing Ongoing Ongoing

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
		Hospitality and employees are required to report these using the Gifts & Hospitality Tool. The payment of ex-gratia payments or legal settlements are strictly controlled and must be submitted to the Group Legal Director for approval. Post Office has a Group wide training programme to ensure that all customer facing staff, back office staff and contractors receive adequate training. Staff and contractors are required to complete training within 30 days of joining Post Office and annually.	any offers of gifts or hospitality over the agreed amounts Financial Crime Team is responsible for reviewing and monitoring the Gifts and Hospitality register Group Legal Director is responsible for reviewing and signing off as required any ex-gratia payments or legal settlements as requested from the Business. Human Resources is responsible for any incidents where further action is required and ensuring completion of mandatory training	Ongoing Ongoing
Political Donations/Lobbying	Employees making or soliciting political donations on behalf of Post Office may result in criminal prosecution.	Preventative Control: Before giving or offering Hospitality to or from a political party, approval must be obtained from a GE Member. The giving of political donations or gifts on behalf of the group to a Politician or a Political Party is~~are~~ strictly prohibited.	Each employee is responsible for ensuring that all Gifts & Hospitality offered or received is recorded Group Executive are~~is~~ responsible for the approving or declining of any offers of hospitality by a political party	Ongoing Ongoing

POL00401627

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
		Post Office has a Group wide training programme to ensure that all customer facing staff, back office staff and contractors receive adequate training. Staff and contractors are required to complete training within 30 days of joining Post Office and annually.	Financial Crime Team is responsible for reviewing the Gifts and Hospitality register Human Resources is responsible for any incidents where further action is required and ensuring completion of mandatory training	Ongoing
Procurement/Third Party Risk	Inadequate monitoring may lead to third parties engaging in bribery or corruption while performing services on behalf of the Post Office Group. This could result in criminal prosecution, loss of key contracts or reputational damage.	Preventative Control: Post Office ensures that any fees paid are proportional to the services being rendered or consistent with the market. New and existing contracts are reviewed on an ongoing basis to ensure that there is no risk of conflicts of interest. This includes ensuring that all parties involved are aware of Procurement Lockdowns.	Chief Financial Officer Procurement	Ongoing Ongoing

The Group completes Annual Risk Assessments reviewing its bribery and corruption exposure and its compliance with the above key risk areas.

3. Definitions

3.1. Definitions

Bribery
Bribery is defined as the offer, promise, payment, request, agreement to receive anything of value whether directly or indirectly to or from any person or entity in order to induce that person or entity to perform their roles improperly or, in the case of a Public Official, in order to influence them with the intention of obtaining or retaining business or an advantage in the conduct of business.

Examples include an offer or promise to give anything of value to anyone to obtain or retain business for or on behalf of the Post Office or to obtain or fulfil a legal or regulatory requirement in furtherance of the Group's business. A bribe can take the form of a "reward" and be paid after the improper performance of the relevant duty or obligation.

Corruption
Corruption is defined as the misuse of entrusted power or public office for private gain.

Educational courses/conferences
Events that are offered by third parties without charge do not amount to hospitality. However, free places to attend courses or conferences that would otherwise attract a charge are covered by this procedure.

Facilitation Payment
A Facilitation Payment is a type of bribe and should be seen as such. A common example is where a government official is given money or goods to perform (or speed up the performance of) an existing duty. Within the UK these are strictly prohibited.

Gifts
Gifts refers to a physical gift and includes the offer to a specific individual or team with the exception of low value promotional items costing under £20 each, such as pens, calendars, diaries, notepads and paperweights.

Hospitality
Invitations to attend events which have a social element (whether or not they are at the same time as or linked to a business meeting) and where the cost of a 'ticket' (participation) is free of charge or reduced in price when otherwise there would be cost attached to it. This would include things such as tickets to a sporting event, tickets to a concert or a corporate dinner.

Inducement
An inducement is a benefit offered to a firm or any person acting on its behalf, with a view to that firm, or that person, adopting a particular course of action. This can include, but is not limited to, cash, cash equivalents, commission, goods, hospitality or training programmes.

Third Party funded trips
Travel/accommodation that is funded by third parties is covered by this procedure as a form of 'hospitality'.

4. Where to go for help

4.1. Additional Policies

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

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

4.2. How to raise a concern

Any Post Office employee who suspects that there is a breach in this Policy should report this without any undue delay.

In case of bribery or corruption concerns or whistleblowing, staff may contact:

- their line manager,
- a senior member of the HR Team, or
- if either or both are not available, staff can contact the Post Office's General Counsel, who can be contacted by email at: whistleblowing GRO or by telephone on: GRO
- Alternatively staff can use the Speak Up service available on GRO
- or via a secure on-line web portal: http://www.intouchfeedback.com/postoffice

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

4.3. Who to contact for more information

If you need further information about this Policy or wish to report an issue in relation to this Policy, please contact the Policy sponsor or Policy owner.

5. Governance

5.1. Governance Responsibilities

The Policy sponsor, responsible for overseeing this Policy is the General Counsel of Post Office Limited.

The Policy owner is the Director of ~~Risk and~~ Compliance who is responsible for ensuring that the Financial Crime Team conducts an annual review of this Policy and tests compliance across the Group. Additionally the Director of ~~Risk and~~ Compliance and the Financial Crime Team are responsible for providing appropriate and timely reporting to the Risk and Compliance Committee and the Audit and Risk Committee.

The Audit and Risk Committee are responsible for approving the Policy and overseeing compliance.

The Board is responsible for setting the Group's risk appetite.

6. Control

6.1. Policy Version

Date	**Version**	**Updated by**	**Change Details**
November 2016	1	Georgina Blair	Roll out of Final version
June 2017	1.2	Thomas Richmond	Updated in line with comments from stakeholders
July 2017	1.3	Sally Smith	POL R&CC approval
September 2017	2	Sally Smith	Final Version approved by ARC
June 2018	2.1	Sally Smith	Annual revisions

6.2. Policy Approval

Group Oversight Committee: Risk and Compliance Committee and Audit and Risk Committee

Committee	**Date v 2.0 Approved**
POL R&CC	20th July 2017
POMS R&CC	31st August 2017
POMS ARC	18th September 2017
POL ARC	25th September 2017

Policy Sponsor: Group Director of Legal, Risk & Governance

Policy Owner: Director of ~~Risk and~~ Compliance

Policy Author: Head of Financial Crime

Next review: ~~August 2018~~June 2019

Company Details

Post Office Limited and Post Office Management Services Limited are registered in England and Wales. Registered numbers 2154540 and 08459718 respectively. Registered Office: Finsbury Dials, 20 Finsbury Street, London EC2Y 9AQ.

Post Office Management Services Limited is authorised and regulated by the Financial Conduct Authority (FCA), FRN 630318. Its Information Commissioners Office registration number is ZA090585.

Post Office Limited is authorised and regulated by Her Majesty's Revenue and Customs (HMRC), REF 12137104. Its Information Commissioners Office registration number is Z4866081.

Whistleblowing Policy

Author: Sally Smith Sponsor: Jane MacLeod Meeting Date: 10th July 2018

Executive Summary

Context

This paper sets out the updates and revisions to the Whistleblowing Policy as part of the annual review process for the Risk and Compliance Committee to consider and approve.

Questions addressed in this paper

- What changes to the Policy do we propose and why?
- What are the implications of these changes?

Conclusion

1. The Whistleblowing Policy has been amended to clarify the minimum control standards, roles and responsibilities
2. There are some minor changes to the requirements and minimum standards of controls which will be communicated to relevant stakeholders

Input Sought

The R&CC is asked to approve the updated Whistleblowing Policy.

The Report

Why do we need to review this Policy?

1. The Policy was last reviewed and approved by the R&CC in September 2017. The terms of the Policy require it be reviewed annually.

What changes to the Policy do we propose and why?

What are the key features that we propose and why?

2. There have been no legislation changes in the past year and no significant amends made to the policy at this annual review.
3. Minor amends have been made in relation to:
   - Revised definition of serious incidents in section 1.3
   - Updated with new link for Speak Up web portal
   - Added communication and awareness to all staff as minimum control standards
   - Included reference to Whistleblowing Officer nominated deputies to minimum control standards

How did we develop these recommendations?

4. Policy queries and issues that have arisen over the previous 12 months have been reviewed to ensure that these concerns are addressed.

What are the implications of these changes?

What will we need to do and by when, to implement and embed these Policy changes?

5. No material changes are required to comply with this updated Policy.
6. Internal communications and training – once the Policy has been approved, there will be a One communication to advise all employees of the changes and provide a link to the updated document on the Post Office Intranet.

What will the impact be on our wider business?

7. Transparency of Post Office's adherence and commitment to the Employment Rights Act 1996 and the Public Interest Disclosure Act 1998
8. The Financial Crime Team monitor adherence to the minimum control standards set out in the Policy on an on-going basis through their review of the Gifts and Hospitality Tool and any other reported issues - any control gaps identified are reported to the R&CC as required. Appendix A provides an overview of the assurance checks developed by the Financial Crime team during 2017/18.

What would the impact be of delaying approval?

9. Risk that the group breaches the Employment Rights Act 1996 and the Public Interest Disclosure Act 1998 by not having up to date policies and procedures to provide protections to whistleblowers.
10. Post Office Limited is required to maintain up to date policies to support contractual requirements with clients and suppliers (e.g. MoneyGram and the Partner Banking Framework) and failure to do so may result in a breach of contract, and whilst not material, could have commercial and reputational impacts.

11. Post Office Limited provides Post Office Management Services (POMS) with its policies suite in the form of "Group Policies". POMS is required under its regulatory responsibility to the Financial Conduct Authority to have up to date policies and failure to do so may lead to regulatory sanctions or penalties.

POL00401627

Appendix A - Minimum Control Standards Assurance

The below table shows the residual risk rating from a first and second line of defence perspective for each control type within the currently approved policy as at the Q1 2018/19 review

Risk Description	Control Type	Description of control	Residual risk rating			Control Strength		Q1 Assurance Comments
			L	I	S	1st LoD	2nd LoD	
Failing to investigate the whistleblowing report and take necessary action	Directive	(a) Nomination of a Whistleblowing Officer; (b) Regular reports to R&CC/ ARC; (c) Escalation process to the Audit and Risk Committee	1	2	2	Effective	Effective	Whistleblowing log spreadsheet maintained and monitored by Whistleblowing Officer and Financial Crime Team to ensure all investigations complete. Summary reports provided to R&CC and ARC regularly.
Failing to investigate the whistleblowing report and take necessary action	Preventative	(a) WB Policy; (b) training; (c) Escalation of WB reports; (d) comms	1	2	2	Effective	Effective	Whistleblowing comms launched in May, posters at all customer support centres, supply chain and DMBs. Intranet/One Article and DMB branch focus.
Failure to ensure confidentiality for the whistleblower	Preventative	(a) WB policy; (b) Speak Up line reporting; (c) designated WB email inbox; (d) WB confidentiality arrangements	1	2	2	Effective	Effective	Access to systems restricted to Whistleblowing officer and nominated deputies. Documented process is currently being reviewed and re-drafted. Details regarding Whistleblowing found on 'My HR' page are being updated.
Failure to ensure confidentiality for the whistleblower	Corrective	(a) WB breach escalation process	1	2	2	Effective	Effective	Only Whistleblowing Office and nominated deputies have access to reports. Where these need to be referred to other parties to initiate investigations then a standard confidentiality statement and instructions are included in the request.
An individual may raise a whistleblowing report with other individuals in the Group. Details may then be shared with various stakeholders before being passed onto the Whistleblowing Officer	Preventative	(a) WB policy; (b) training; (c) comms.	1	2	2	Effective	Effective	Training provided to Grapevine, NBSC, Customer Support and ECT August 2017 and additional comms have been undertaken since. Plan to provide further training during Q2.

Risk Description	Control Type	Description of control	Residual risk rating			Control Strength		Q1 Assurance Comments
			L	I	S	1st LoD	2nd LoD	
An individual may raise a whistleblowing report with other individuals in the Group. Details may then be shared with various stakeholders before being passed onto the Whistleblowing Officer	Corrective	(a) WB breach escalation process	1	2	2	Effective	Effective	There have been no incidents where potential WB reports have not been sent to the Whistleblowing Officer, and further comms planned that will reinforce requirements
Failure to capture/report sufficient information about the issue may mean that the underlying issue cannot be properly investigated and resolved	Directive	(a) WB policy; (b) training.	2	2	4	Effective	Effective	Posters are on display at all back office sites and directly managed branches explaining to staff when and how to report. Additionally, Paula Vennals blog covered Whistleblowing and promoted the 'Speak Up' Line. My HR help page still directs employees to an out of date Whistleblowing policy' we are chasing to get this resolved. ABC Training due at end July and will incorporate whistleblowing awareness.
Failure to capture/report sufficient information about the issue may mean that the underlying issue cannot be properly investigated and resolved	Corrective	(a) Review of WB report database	2	2	4	Effective	Effective	There has only been one reporter where there was insufficient detail, this was reported by the Speak Up portal and they were requested to provide further information if they wished us to investigate. All reporters encouraged to give as much information as possible.
Failure to effectively record whistleblowing reports and pass onto the Whistleblowing Officer, due to factors such as resource or IT failure	Preventative	(a) Review of service and processes; (b) WB policy	1	2	2	Effective	Effective	Contract with InTouch Ltd has been reviewed (Now called Expolink Europe Ltd). There have been some enhancements to the services and reporting that they provide to their clients. No issues identified with provider. Internal processes will be reviewed over the next quarter.
Breach of whistleblowing guidelines such that a whistleblower suffers	Preventative	(a) WB policy; (b) training; (c) comms.	1	2	2	Effective	Effective	ABC training due end of July, will include WB.

Risk Description	Control Type	Description of control	Residual risk rating			Control Strength		Q1 Assurance Comments
			L	I	S	1st LoD	2nd LoD	
prejudice as a result of making a report								

POST OFFICE

GROUP POLICIES

Whistleblowing Policy

Version – V2.1

Chief Executive's Endorsement

The Post Office Group is committed to doing things correctly. Our Values and Behaviours represent the conduct we expect. This Policy supports these to help us ensure that colleagues know how to report concerns regarding wrongdoing or dangerous practices and that they can do so without fear of recrimination.

1. Overview

1.1. Introduction by the Policy Owner

The General Counsel has overall accountability to the Board of Directors for the implementation of controls ensuring Post Office meets it Whistleblowing obligations. Whistleblowing is an agenda item for the Audit and Risk Committee and the Post Office board is updated as required.

1.2. Purpose

This Policy has been established to set the minimum operating standards relating to the management of Whistleblowing throughout the Group[1]. It is one of a set of policies which provide a clear risk and governance framework and an effective system of internal control for the management of risk across the Group. Compliance with these policies supports the Group in meeting its business objectives and to balance the needs of shareholders, employees[2] and other stakeholders.

1.3. Core Principles

Whistleblowing is the reporting of suspected wrongdoing and/or dangerous practices within[SS1] Post Office. This would include serious accidents, bribery, fraud, any criminal activity, regulatory breaches, miscarriages of justice, health and safety risks, damage to the environment, financial impropriety~~ and/or~~, reputational damage and/or any breach of legal or professional obligations.

In order to encourage Whistleblowing and provide appropriate protections to whistleblowers, the governance arrangements described in this Policy are based upon the following core principles:

- To encourage the reporting of any concerns as soon as possible in the knowledge that all concerns will be taken seriously and investigated, and that confidentiality will be respected;
- To provide guidance as to how to raise those concerns;
- To provide whistleblowers reassurance that all concerns are raised without fear of reprisals, even if they turn out to be mistaken;
- Post Office is committed to and oversees the implementation of a Policy in line with the Group's risk appetite. The Policy and associated procedures (set out or referred to in this document) are proportionate to the risks and complexity of the Group;
- Post Office undertakes a training and awareness program to ensure employees are aware of the Whistleblowing policy and procedure.

1.4. Application

This Policy is applicable to all employees within the Group and outlines the protections provided for whistleblowers by law. In order to encourage reporting of wrongdoing, Post

[1] In this Policy "Post Office" and "Group" mean Post Office Limted and Post Office Management Services Limited.
[2] In this Policy "employee" means permanent staff, temporary including agency staff, contractors, consultants and anyone else working for or on behalf of Post Office.

Office will, where appropriate, extend equivalent protection to Postmasters, Agent Assistants, and members of the public.

1.5. Legislation

The Group seeks to comply with all relevant UK legal and regulatory requirements including (but not limited to) the following legislation as amended or supplemented from time to time:

- Employment Rights Act 1996
- Public Interest Disclosure Act 1998

1.6. What is Whistleblowing

"Whistleblowing" refers to the act of exposing potential or actual wrongdoing and/or dangerous practices by reporting it either internally within an organisation, or to an external party. A whistleblower is a person who raises a genuine concern in relation to any wrongdoing, this includes criminal activity, miscarriages of justice, dangers to health and safety and the deliberate attempt to conceal it.

Individuals[3] should raise a concern if they are aware of, or suspect, wrongdoing which affects others (e.g. customers, members of the public, colleagues or the Post Office). The following lists some examples (this is a non-exhaustive list) of situations where an individual may raise a concern:

- Financial Crime including Fraud, Money Laundering and financing of terrorism,
- Giving, offering or taking of bribes,
- Financial mismanagement,
- Misreporting,
- Practices that could put individuals or the environment at risk,
- Breach of Post Office internal policies and procedures (including the Code of Business Standards),
- Tax Evasion,
- Concerns about slavery or human trafficking[4], and
- Any conduct likely to damage Post Office's reputation

Grievances and matters such as bullying and harassment are addressed under Post Office's HR policies and concerns in relation to such matters should be raised in accordance with the procedures set out in the appropriate HR policy.

If an individual is uncertain about whether something is within the scope of this Policy they should seek advice from the Whistleblowing Officer, whose contact details are set out in this Policy.

1.7. Protecting the whistleblower

Post Office has a statutory obligation to protect whistleblowers and will support any individual who raises genuine concerns under this Policy, even if they turn out to be mistaken. Post Office are committed to respecting the confidentiality of all whistleblowers, ~~and~~ including those who wish to remain anonymous.

[3] In this Policy "individuals" means Postmasters, Agent Assistants, members of the public and employees (permanent staff, temporary including agency staff, contractors, consultants and anyone else working for or on behalf of Post Office). The statutory protections offered under the Public Interest Disclosure Act 1998 only apply to employees, however Post Office Limited will consider extending these protections to other individuals where they have acted in good faith in raising concerns

[4] More information in relation to Modern Slavery can be found here - http://corporate.postoffice.co.uk/slaverystatement

Post Office will make every effort to protect the whistleblowers identity, however, it may be necessary in the course of an investigation to share this information with a relevant stakeholder (e.g. an investigator). There is no requirement for a whistleblower to provide personal contact information. However, not providing this information may reduce Post Office's ability to undertake a thorough investigation into the concerns raised.

Post Office will take all reasonable steps to ensure that whistleblowers do not suffer any detrimental treatment as a result of raising a concern. Detrimental treatment includes disciplinary action, dismissal, threats or other unfavourable treatment connected with raising a concern. Serious action will be taken against any individual who threatens or retaliates against whistleblowers in any way.

If an individual believes that they have suffered any such treatment, they should inform the Whistleblowing Officer immediately. The Whistleblowing Officer should take steps to address any victimisation, which may include working with the HR team to put appropriate measures in place. If the matter is not addressed the whistleblower should raise it formally using Post Office's Grievance procedure.

In all cases the individual's concerns will be treated sensitively and in confidence.

1.8. Whistleblowing Officer and 'Speak Up'

Post Office has ~~a~~ appointed the General Counsel as the Whistleblowing Officer who can be contacted on whistleblowing GRO

The Whistleblowing Officer will review concerns raised and determine the best course of action, if any. They may ask for further information in order to make this decision.

It is recognised that sometimes raising a concern directly with the business may not be possible. In such instances individuals should contact the "Speak Up" line, a confidential reporting service which is run by an independent company Expolink Europe Ltd (formerly known as InTouch MCS Ltd).

Contact details for the Speak Up line are:

- GRO
- https://wrs.expolink.co.uk/postoffice ~~http://www.intouchfeedback.com/postoffice~~ which is a secure on-line web portal[SS2]:

All reports to the Speak Up line will be acknowledged within five working days and will be passed to the Whistleblowing Officer.

It is also possible that individuals may whistleblow via a complaint to a front line team, e.g. Customer complaints, NBSC and Grapevine. These may be verbal or written communications.

In all instances any whistleblowing reports, regardless of reporting method, will be passed onto the Whistleblowing Officer. The whistleblower may be kept informed of any action taken, however, this information may be limited if it is required to keep the confidence of other people.

1.9. External Disclosures

The aim of this Policy is to provide an internal mechanism for reporting, investigating and remedying any wrongdoing in the workplace. In most cases individuals should not find it necessary to alert anyone externally.

However, the law recognises that in some circumstances it may be appropriate for individuals to report their concerns to an external body such as a regulator. The independent Whistleblowing charity, Public Concern at Work have a list of prescribed regulators for reporting certain types of concerns. Their contact details are as follows:

Helpline GRO
E-mail: whistle GRO
Website: www.pcaw.co.uk

Public Concern at Work operates free, confidential advice to people concerned about crime, danger or wrongdoing in the workplace. Post Office strongly encourages advice is sought out from Public Concern at Work before reporting any concern to an external party.

Post Office Money Services (POMS) is directly regulated by the Financial Conduct Authority (FCA), Post Office Limited is an appointed representative of Bank of Ireland (UK) Limited. As such individuals may decide to whistleblow directly to the FCA, and can do so by using one of the following channels.

Helpline: GRO
E-mail: whistle GRO
Website: www.fca.org.uk/site-info/contact/whistleblowing
Address: Intelligence Department (Ref IDA), Financial Conduct Authority, 25 the North Colonnade, London E14 5HS

2. Risk Appetite and Minimum Control Standards

2.1. Risk Appetite

Risk Appetite is the extent to which the Group will accept that a risk might happen in pursuit of day to day businesses transactions. It therefore defines the boundaries of activity and levels of exposure that the Group are willing and able to tolerate.

The Group takes its legal and regulatory responsibilities seriously and consequently has[5]:

- **Tolerant risk appetite** for Legal and Regulatory risk in those limited circumstances where there are significant conflicting imperatives between conformance and commercial practicality
- **Averse risk appetite** for litigation in relation to high profile cases/issues
- **Averse risk appetite** for ligation in relation to Financial Services matters
- **Averse risk appetite** for not complying with law and regulations or deviation from business' conduct standards for financial crime to occur within any part of the organisation
- **Averse Risk Appetite** in relation to unethical behaviour by our staff.

The Group acknowledges however that in certain scenarios even after extensive controls have been implemented an action may still sit outside the agreed Risk Appetite.

2.2. Policy Framework

Post Office has established a suite of policies and procedures, on a risk sensitive approach which are subject to an annual review. The policy suite is designed to comply with applicable legislation and regulation. The Whistleblowing Policy should be considered and read in conjunction with other policies where relevant. These may include the Financial Crime Policy, the Anti-Bribery & Corruption Policy, Health & Safety Policies and HR Policies where relevant.

2.3. Who Must Comply?

All third parties who do business with the Group, including consultants, suppliers and business and franchise partners, will be required to agree contractually to this policy or have their own equivalent policy.

Any investigations will be carried out in accordance with the Investigations Policy which is available on the Post Office Intranet

[5] The Risk appetite was agreed by the Groups Board January 2015

2.4. Minimum Control Standards

A minimum control standard is an activity which must be in place in order to manage the risks so they remain within the defined Risk Appetite statements. There must be mechanisms in place within each impacted business unit to demonstrate compliance. The minimum control standards can cover a range of control types, i.e. directive, detective, corrective and preventive which are required to ensure risks are managed to an acceptable level and within the defined Risk Appetite.

The table below sets out the relationships between identified risk and the required minimum control standards in consideration of the stated risk appetite. The subsequent pages define the terms used in greater detail:

Risk Area	**Description of Risk**	**Minimum Control Standards**	**Who is responsible**	**When**
Receipt and investigation of whistleblowing reports	Failure to meet legal and regulatory requirements	Directive Control: Post Office must nominate a Whistleblowing Officer to receive reports, ensure that all reports are fully investigated and that any appropriate corrective action is undertaken.	Post Office CEO and Board	Ongoing
		The whistleblowing officer must provide a whistleblowing report to the R&CC and ARC at least annually.	Whistleblowing Officer	Annually
		Any serious whistleblowing concerns must be promptly escalated to the Chairman of the Post Office Audit and Risk Committee.	Whistleblowing Officer	Ongoing
		Preventative Control: All employees are trained and the policy is available to them	Whistleblowing Officer	Training must be provided at least annually

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
		The Whistleblowing Officer must ensure that appropriate arrangements are in place to ensure that whistleblowing reports are addressed promptly including during absences Communications and awareness provided to all employees and Policy document published on the Intranet[SS3].	Whistleblowing Officer Head of Financial Crime	Ongoing Annually
Breach of confidentiality	Failure to ensure confidentiality for the whistleblower	Preventative Control: Whistleblowing Policy Confidential Speak Up line reports are shared only with the Whistleblowing Officer and nominated deputies[SS4] Whistleblowing email inbox with access restricted ~~access~~to the Whistleblowing Officer and nominated deputies Whistleblowing Officer must put arrangement in place to protect the confidentiality of the whistleblower during investigations Corrective Control: All incidents of breaches are escalated to the Whistleblowing Officer to review and take necessary actions.	Whistleblowing Officer Whistleblowing Officer Whistleblowing Officer Whistleblowing Officer Whistleblowing Officer	Ongoing Ongoing Ongoing Ongoing Ongoing

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
Incorrect handling of whistleblowing report	An individual may raise a whistleblowing report with other individuals in the Group. Details may then be shared with various stakeholders before being passed onto the Whistleblowing Officer	Preventative Control: Training provided to contact teams to identify potential whistleblowing reports and ensure these are correctly handled, e.g.: • Grapevine, • NBSC, • Customer Support, and • Executive Complaints.	Whistleblowing Officer	Annually
		Communications and awareness provided to all employees and Policy document published on the Intranet.	Head of Financial Crime	Annually
		Corrective Control: All incidents of breaches are ~~be~~ escalated to the Whistleblowing Officer to investigate and take appropriate actions.	Whistleblowing Officer	Ongoing
Insufficient Information	Failure to capture/report sufficient information about the issue may mean that the underlying issue cannot be properly investigated and resolved	Directive Control: Employees are encouraged to report issues and provide full information and their contact details, where they feel able to do so	Whistleblowing Officer	Ongoing
		Corrective Control: All reports, including those where insufficient information has been provided and no further action was taken are recorded on the Whistleblowing	Whistleblowing Officer	Ongoing

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
		database, which is reviewed for trends and issues.		
The 'Speak Up' Service	Failure to effectively record whistleblowing reports and pass onto the Whistleblowing Officer, due to factors such as resource or IT failure.	Preventative Control: The Whistleblowing Officer must review the effectiveness of the service provided by Expolink Europe Ltd (formerly known as InTouch MCS Ltd) ~~InTouch Ltd~~ at least annually The Whistleblowing Officer must review the effectiveness of the processes operated by each of Grapevine, NBSC, Customer Support, and The Executive Complaints Team at least annually to ensure that whistleblowing reports are identified and communicated promptly.	Whistleblowing Officer Whistleblowing Officer	Annually Annually
Treatment of Whistleblowers	Breach of whistleblowing guidelines such that a whistleblower suffers prejudice as a result of making a report	Preventative Control Training must be provided to all people managers as part of their induction process as a manager and on appointment to Post Office Annual training must be provided to all Post Office staff to remind them of the protections available to whistleblowers and the	Whistleblowing Officer and HR Training Manager Whistleblowing Officer and HR Training Manager	Ongoing Ongoing

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
		importance of identifying and reporting wrongdoing The Code of Business Standards must refer to the whistleblowing policy and must be provided to all new joiners as part of their induction programme.	Whistleblowing Officer and HR Training Manager	Ongoing

3. Definitions

3.1. Definitions

Grapevine
24/7 Security Support Centre provided by Kings Ltd. Grapevine provide security advice and record all security incidents across the business, this includes burglaries, robberies and the reporting of suspicious activity.

Telephone Number: GRO
E-mail: grapevine.admin GRO

NBSC
Network Business Support Centre (NBSC) is a helpline and the first port of call for Post Office branches if they have any operational query or require assistance.

Telephone Number: GRO
E-mail: nbscenquiries GRO

Customer Support Team
Complaints handling team based in Chesterfield. The team address complaints reported into Post Office via various channels, including post and telephone.

E-mail: customercare GRO

Executive Complaints Team
This team handles all complaints addressed directly to the Group Executives. The team liaise with various stakeholders within the business in order to resolve complaints.

E-mail: flagcaseadvisor GRO

4. Where to go for help

4.1. Additional Policies

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

https://poluk.sharepoint.com/sites/thehub/SitePages/Key%20policies.aspx?web=1 ~~https://poluk.sharepoint.com/sites/postoffice/Pages/policies.aspx~~

4.2. How to raise a concern

Any Post Office employee who suspects that there is a breach of~~in~~ this Policy should report this without any undue delay. Whistleblowing can be reported via the following channels:

- Their line manager,
- A senior member of the HR Team, or
- If either or both are not available, staff can contact the Post Office's Whistleblowing Officer, who can be contacted by email at: whistleblowing GRO or by telephone on: GRO
- Alternatively staff can use the Speak Up service available on GRO or via the secure on-line web portal: https://wrs.expolink.co.uk/postoffice ~~http://www.intouchfeedback.com/postoffice~~

In some instances it may be appropriate for the individual to report in the form of a complaint to Grapevine, the Customer Support Team or the Executive Complaints Team.

4.3. Who to contact for more information

If you need further information about this Policy or wish to report an issue in relation to this Policy, please contact the Policy sponsor or Policy owner.

5. Governance

5.1. Governance Responsibilities

As at the date of approval of this Policy, the General Counsel is both the Policy Sponsor and Policy Owner, responsible for oversight of the Policy.

The Audit and Risk Committee are responsible for approving the Policy and overseeing compliance.

The Board is responsible for setting the Group's risk appetite.

6. Control

6.1. Policy Version

Date	Version	Updated by	Change Details
April 2016	1.4	Jane MacLeod	Sponsors review and sing-off
August 2017	1.5	Vitor Camara	Annual Review and update.
September 2017	1.6	Thomas Richmond	POL R&CC approval
September 2017	2	Thomas Richmond	Final version approved
June 2018	2.1	Vitor Camara	Annual review and update.

6.2. Policy Approval

Group Oversight Committee: Risk and Compliance Committee and Audit and Risk Committee

Committee	Date version 2.0 Approved
POL R&CC	13th September 2017
POMS R&CC	31st August 2017
POMS ARC	18th September 2017
POL ARC	25th September 2017

Policy Sponsor: Group Director of Legal, Risk & Governance

Policy Owner: Whistleblowing Officer

Policy Author: Head of Financial Crime

Next review: ~~August 2018~~July 2019

Company Details

Post Office Limited and Post Office Management Services Limited are registered in England and Wales. Registered numbers 2154540 and 08459718 respectively. Registered Office: Finsbury Dials, 20 Finsbury Street, London EC2Y 9AQ.

Post Office Management Services Limited is authorised and regulated by the Financial Conduct Authority (FCA), FRN 630318. Its Information Commissioners Office registration number is ZA090585.

Post Office Limited is authorised and regulated by Her Majesty's Revenue and Customs (HMRC), REF 12137104. Its Information Commissioners Office registration number is Z4866081.

Whistleblowing Annual Report 2017-18

Author: Sally Smith

Sponsor: Jane MacLeod

Meeting Date: 10th July 2018

Executive Summary

Context

This report provides an overview of the financial year 2017/18 as part of our obligations to protect whistleblowers and support individuals who raise genuine concerns under the Whistleblowing Policy. The report provides a summary of the activities undertaken to raise awareness and evidence that all reports are properly investigated.

Questions addressed in this paper

- What issues have been highlighted based on the review?
- What actions need to be undertaken to mitigate any issues identified?

Conclusion

1. The whistleblowing reports received have not identified any significant areas of concerns nor do they indicate any systemic problem within the Post Office. The majority have been from agents or agent assistants, which Post Office treats in the same way as employees under the Employment Rights Act 1996 and the Public Interest Disclosure Act 1998.

2. A complete review of whistleblowing reporting channels and processes has been undertaken to enhance controls and business communication and awareness has improved.

Input Sought

The RCC are asked to review the contents of this report and advise any further actions required.

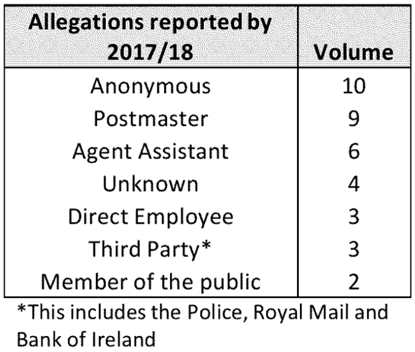
The Report

Summary of activities relating to Whistleblowing reporting 2017-18

1. The whistleblowing policy was reviewed, updated and approved in September 2017.
2. During 2017-18, the Whistleblowing Officer appointed as nominated deputies, individuals within the Financial Crime Team to monitor and manage whistleblowing reports and investigations on a day to day basis.
3. A review of the whistleblowing process and report log was conducted by the Financial Crime team to ensure compliance with policy. As a result a number of historic cases were reviewed and closed, and training and guidance was given to NBSC, Grapevine, the Executive Complaints Team and Customer Support to help them identify any complaints that should be reported to the Whistleblowing Office and treated accordingly.
4. New processes have been implemented to ensure that those parties within Post Office who have to be involved in investigations into allegations are fully aware of their responsibilities and the confidential nature of their investigations.
5. Access rights were reviewed for the Whistleblowing Mailbox and the Speak Up Line portal to ensure access was appropriate.
6. The Speak Up service was promoted through both Paula's blog and the February 2018 Team Talk Plus.
7. The contract with ExpoLink Europe Ltd (formerly InTouch MCS Ltd), provider of the Speak Up service has been reviewed and was due for renewal in April 2018. This is being renewed, together with a contract variation to comply with recent GDPR changes.

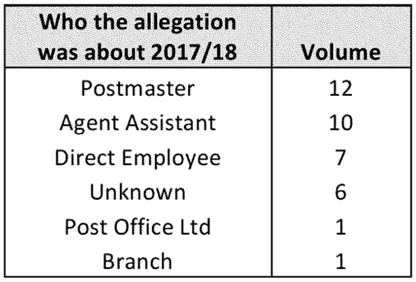
Summary of Whistleblowing reports received 2017-18

8. During 2017-18, 37 whistleblowing reports were received and 33 cases were closed.
9. The majority of the allegations were about Postmasters or Agent Assistants (22 reports). There were 7 reports made about Post Office employees.



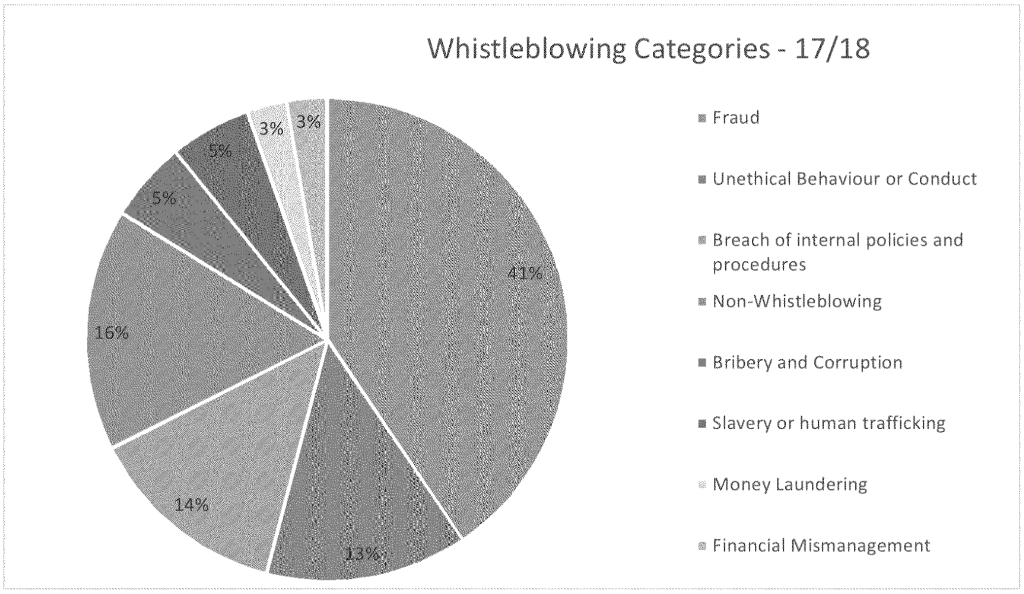
Allegations reported by 2017/18	Volume
Anonymous	10
Postmaster	9
Agent Assistant	6
Unknown	4
Direct Employee	3
Third Party*	3
Member of the public	2

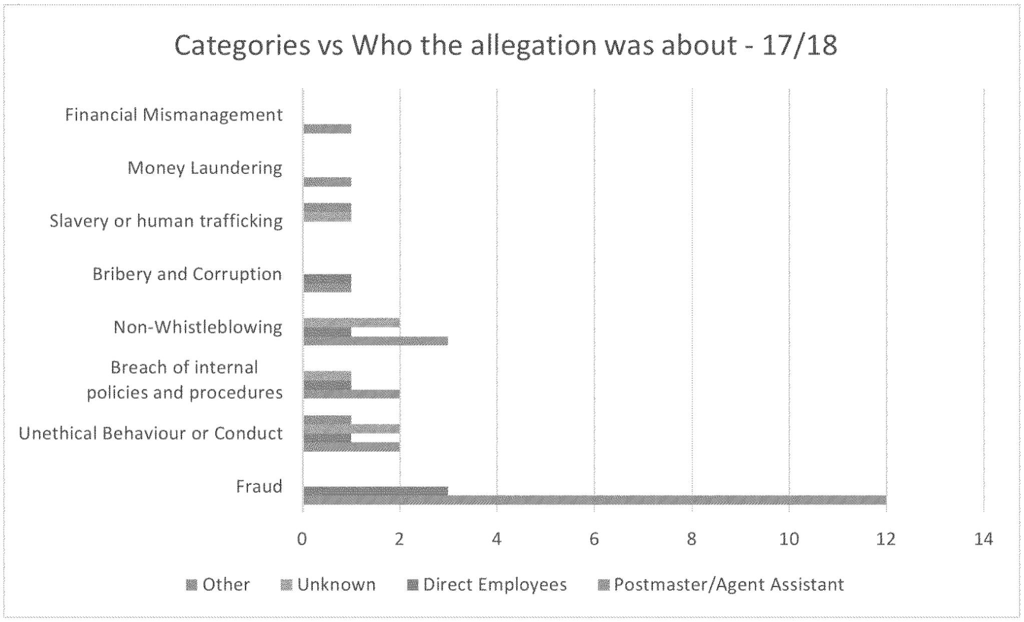
*This includes the Police, Royal Mail and Bank of Ireland



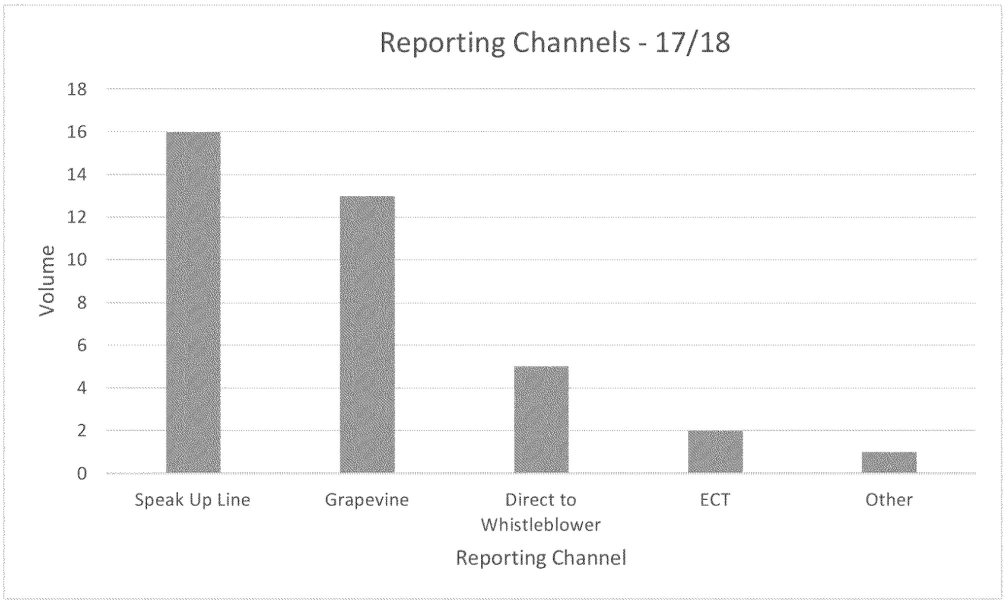
Who the allegation was about 2017/18	Volume
Postmaster	12
Agent Assistant	10
Direct Employee	7
Unknown	6
Post Office Ltd	1
Branch	1

10.41% of the reports received were allegations of fraud. Predominately this was about either a Postmaster or Agent Assistant (12), however, there were 3 reports involving Post Office employees.





12.The most popular channels used to report concerns were the Speak Up line (16) and Grapevine (13).



13.The whistleblowing reports have not identified any route cause which may indicate a systemic problem. However, some investigations have led to further issues being identified at branches and appropriate corrective action has been taken. This includes temporary suspensions of Postmasters.

Activities planned for 2018-19:

1. A communications campaign went live at the start of 2018-19 and this has so far included a Branch Focus Article for DMBs, an Intranet Article, Yammer posts and whistleblowing awareness posters at all Customer Support Centres, Supply Chain sites and DMBs.
2. The following activity is planned:

- Continuous communications and awareness.
- Whistleblowing Policy annual review and update July 2018
- Expolink Europe Ltd (InTouch MCS Ltd) contract renewal to be finalised.
- Process documents across all areas to be reviewed and updated.
- The Financial Crime Team to review the functionality and performance of the Expolink Ltd case management system to ensure it meets Post Office requirements and contractual commitments.

Post Office Ltd
POST OFFICE LIMITED RISK AND COMPLIANCE COMMITTEE
10 July 2018

Location:

The Boardroom, Wakefield (1.19), Finsbury Dials, 20 Finsbury Street, London, EC2Y 9AQ, United Kingdom

ATTENDANCE LIST

ATTENDEES	SIGNATURE
MacLeod, Jane	
Cameron, Alisdair	
Paula, Vennells	

Also in attendance

Koniarski, Sarah	
Houghton, Rob	
Smith, Debbie	
Woodley, Owen	

Additional access

Branton, Veronica	
CoSec	

Post Office Risk and Compliance Committee Agenda

Date	
10 July 2018	
Start Time	**Finish Time**
13.00 hours	16.00 hours
Location	
1.19 Wakefield, Finsbury Dials	

Present	In Attendance		Apologies
Jane MacLeod (Chair) Paula Vennells Al Cameron Meredith Sharples Tom Moran	Jenny Ellwood Johann Appel Jonathan Hill Paul Beaumont David Meldrum Barbara Brannon Sally Smith	Sarah Koniarski (Secretary) Lisa Toye (Secretary)	

Agenda Item	Action Needed	For ARC	Purpose	Lead	Time
1. Welcome and Conflicts of Interest			Members to declare any conflicts of interest.	Chair	13.00 – 13.05 (5 minutes)
2. Minutes and Action Lists	Approval		To approve the minutes of the meeting held on 2nd May 2018 and update on actions.	Chair	13.05 – 13.10 (5 minutes)
3. Risk Update		✓			13.10 – 13.40 (30 minutes)
3.1 Risk Report	Questions & Noting		To review the risk report.	Jenny Ellwood	
4. Internal Audit		✓			13.40 – 14.00 (20 minutes)
4.1 Audit Report	Questions & Noting		To note the Internal Audit Report for onward submission to the ARC.	Johann Appel	

Post Office Risk and Compliance Committee Agenda (cont.)

Agenda Item		Action Needed	For ARC	Purpose	Lead	Time
5.	**Compliance**		✓			14.00 – 14.45
	5.1 Compliance Report	Noting		To note the Compliance paper	Jonathan Hill	(45 minutes)
	5.1.1 IDD Update	Questions & Noting		Verbal IDD Update	Jonathan Hill	
	5.1.2 PSD2 Update	Questions & Update		Verbal PSD2 Update	Jonathan Hill	
	5.2 Vulnerable Customers Risk Assessment	Input and Discussion			Paul Beaumont	
6.	**Contracts Governance Update**	Input and Discussion		Update on non compliant contracts	Barbara Brannon	14.45 – 14.55 (10 minutes)
7.	**Updates for Noting**					14.55 – 15.10 (15 minutes)
	7.1 PCI-DSS Compliance Status Update	Noting	✓	To note the update on PCI-DSS Compliance Status.	David Meldrum	
8.	**Policies for Approval**		✓	To agree for onward submission to the ARC.		15.10 – 15.30
	8.1 Gifts and Hospitality Policy	Approval			Sally Smith	(20 minutes)
	8.2 Anti-Bribery and Corruption Policy				Sally Smith	
	8.3 Whistleblowing Policy				Sally Smith	
9.	**Future Meetings**	Input and Discussion		Discussion on scheduling and content of future meetings.	Jane MacLeod	15.30 – 15.50 (20 minutes)
10.	**Any Other Business**				Chair	15.50 – 16.00 (10 minutes)
	CLOSE					16.00

Post Office Limited
Risk and Compliance Committee Meeting

MINUTES OF A MEETING OF THE RISK AND COMPLIANCE COMMITTEE (THE "COMMITTEE") OF POST OFFICE LIMITED (THE "COMPANY") HELD ON 2 MAY 2018 AT 20 FINSBURY SREET, LONDON EC2Y 9AQ AT 10.00AM

Present:	Jane MacLeod	Chairman	
	Paula Vennells (PV)	Group Chief Executive	
	Al Cameron (AC)	Chief Financial and Operations Officer	
	Rob Houghton (RH)	Group Chief Information Officer	
	Joe Arakji (JA)	(on behalf of Martin Kirke)	
	Tom Moran (TM)	(on behalf of Debbie Smith)	
	Chrysanthy Pispinis (CP)	(on behalf of Owen Woodley)	
In Attendance:	Jenny Ellwood (JE)	Risk Director	
	Johann Appel (JA)	Head of Internal Audit	
	Jonathan Hill (JH)	Compliance Director	
	Deana Herley (DH)	Senior Assurance Manager	*1 – 3*
	David Gemmell (DG)	GDPR Programme Manager	*6.1–6.2*
	Jules Harris (JH)	Head of Information Protection and Assurance	*6.1-6.2*
	Sarah Koniarski	Secretary	
Apologies:	Debbie Smith (DS)	Chief Executive, Retail	
	Martin Kirke (MK)	Group HR Director	
	Owen Woodley (OW)	Chief Executive, Financial Services and Telecoms	

ACTION

1. WELCOME, INTRODUCTION AND CONFLICTS OF INTEREST

1.1 The Chairman welcomed those present to the meeting and confirmed there was a quorum. There were no conflicts of interest declared.

2. ACTION LIST

2.1 The Action List Status Report was noted as accurate. There were no actions due which had not been addressed in advance of the meeting or through the meeting papers.

3. RISK UPDATE

Top Risks, Executive Declaration and Risk Management Section for ARA

3.1 JE introduced a paper which updated the top risks and executive declaration results. The Committee was asked to review these, together with the draft principal risk statements in the Annual Report and Accounts (ARA) 2017/18. The top risks had been based on feedback from all GE members providing a consolidated view across the Post Office business. The Committee was asked to consider whether any additional disclosures to the principal risks were required for inclusion in the ARA.

3.2 JE provided the following summary:

(a) Referring to the profile of top 12 risks, JE explained that three new top risks had been identified since the half year review: PCI-DSS accreditation; key-man dependency in Banking Services and FS&T; and sustainability of the business model. None of the new risks had created new principal risks, although they did relate to the existing principals.

(b) Three increased risks related to digital competency, safety compliance and business recovery / disaster recovery plan and testing limitations.

(c) Three reduced risks related to technology and business interruption, retail proposition and the ability to achieve "effective" GDPR compliance.

(d) Four risks were no longer deemed top risks but would continue to be managed by the respective teams with responsibility for those areas.

(e) The executive declaration returns had been reviewed by the Group Executive for materiality and consistency against Internal Audit and wider business assurance reviews. The resulting 12 items of materiality were summarised in Appendix 2 to the report. One item of material significance proposed for disclosure in the accounts as a contingent liability was the Post Office Group Litigation. To date, the amount of damages sought was unquantified and a formal state of claim was awaited.

(f) Appendix 3 to the report included an overview of the proposed principal risks mapped against the relevant top risks and executive declarations.

3.3 The following points arose in the ensuing discussion:

(a) FS&T Market Developments / Competition: The Committee reflected on the ongoing negotiations with the Bank of Ireland (BoI). Although BoI was increasingly receptive to agreeing a deal, it remained too early to be confident of securing an agreement which would further Post Office's strategic objectives. It also remained difficult to plot a reliable timeline for delivery. Performance of Financial Services and Telecoms products was a core element of the Annual Operating Plan. The Committee recognised the challenging market conditions which included competitive new entrants together with fast paced advancements in technologies. The Committee agreed that FS&T market developments and competition was a top risk and recommended its ranking be increased accordingly.

(b) Retail Proposition: The Committee was concerned that presenting a decreased risk was not reflective of the present situation. The likelihood of the risk materialising had decreased but its potential impact had increased. The Committee understood that the scoring (which demonstrated likelihood versus impact) would be provided to the Audit, Risk and Compliance Committee ("ARC") but would not be published in the ARA. The Committee asked JE and TM to review its position, with a view to increasing its ranking, before submission to the ARC. TM provided an update on the IRRELEVANT and IRRELEVANT which would result in IRRELEVANT IRRELEVANT A joint working group had made good progress towards increasing their engagement by demonstrating how financial performance could be improved. JE and TM would update the item within the executive declarations to reflect recent developments. It was felt that references to the IRRELEVANT would be better described as IRRELEVANT in the context of recent talks.

(c) Few Key Individuals: It was agreed that any reference to 'key man' dependency throughout be amended to 'key person' dependency and capability. The Committee discussed remedial action including succession planning and providing additional capability. The importance of investing in collective 'bench strength' (increasing individuals' skill sets and subject matter knowledge) was recognised. JA referred to quarterly succession planning meetings and undertook to feedback the Committee's comments on the need to effect cultural change and enable a broader number of reports to gain exposure which would strengthen their skills in preparation for greater ownership of their respective areas.

(d) Safety Compliance: The Committee discussed whether the ranking of risk was reflective of its status. The Committee concurred that the ARA should reflect the importance of safety compliance and demonstrate that it was taken seriously across the organisation, as well as showing the improvements which had been achieved. Accordingly, it was agreed that safety compliance would be maintained as a top risk but renumbered to a lower ranking. JE would work with AC to restructure the comments to demonstrate the encouraging audit findings, the implicit difficulties in managing the risk (due to the wide scope of activities within the business) and the work of Safety Champions to improve performance in Supply Chain.

(e) Sustainability of the Business Model: The Committee agreed to remove the reference to the Group Litigation which was already captured as a separate risk.

(f) FS Regulation: The Committee agreed that AML (Anti-Money Laundering) regulation be highlighted in addition to IDD (Insurance Distribution Directive) requirements.

(g) Agents Pay IT: The Agent Remuneration Transformation (ART) project had completed successfully and was running as business as usual. The Committee understood that agents were being paid through CFS having been migrated from POLSAP and the project-specific risk had closed. There continued to be a risk of not delivering agents' pay which would be monitored as part of business as usual. JE would update the comments to reflect this. The Committee agreed it was appropriate to change the status of this risk to 'closed'.

(h) Royal Mail Industrial Action: The Committee agreed this continued to be a risk and noted that a Post Office internal contingency plan was in place.

(i) Digital Competency: The Committee agreed that this risk should be reallocated as a responsibility shared by the GE with significant support from Human Resources. Following review of the linked proposed principal risks (Appendix 3) it was agreed that digital disruption should be highlighted under the External Environment heading.

(j) DR / BCP Plans: The Committee understood that the comments would be updated in April following tests in Chesterfield and Bolton. AC confirmed that Belfast could not be tested until migration from POLSAP to SAP CFS was completed and Swindon remained a vulnerability. JE would work with AC to update the comments before submission to the ARC. RH added that the lack of support for branches open outside of 'ordinary' business hours (on Sundays for example) was a significant risk to service delivery. Service level agreements did not provide 24 hours' cover meaning there were periods when branches were open without support. RH suggested a gap analysis exercise be carried out to review contractual provisions, identify operational vulnerabilities and determine whether these were within risk appetite or whether mitigating actions were required. RH would discuss the approach with DH.

(k) Emerging risks: The risk of a growing culture of bullying/harassment and the risk of brand erosion (taking account of brand protection and brand relevance) were identified as topics to be explored in future risk work, although no changes to the 2017/18 ARA were recommended. Brand erosion would be explored as part of the rollout of the Placemat in Communications. Further work would also be carried out in relation to Change risk, to identify and mitigate the top risks within the Change programme, including the new 2018/19 plan which would be reviewed for approval by the Investment Committee. Any resulting changes to the risk profile of the Group would be reported to the ARC.

(l) In light of its deliberations, the Committee asked the Chairman to review the descriptions within the principal risks to ensure their emphasis and tone reflected discussion and aligned to the North Star strategy. The Committee suggested that individual reference to Industrial Action under Operational and Financial Risks be removed. A Legal and Regulatory risk pertaining to Group Litigation would be provided as an optional inclusion for ARC to review. Narrative under the External Environment would be expanded and the Committee recommended the Chairman seek the ARC's view on whether an amendment to specify "changes to the interpretation of a workers' status" would be appropriate. The Committee was mindful of references to the Taylor Review (Good work: The Taylor review of modern working practices) included in the Chief Executive's foreword and the materiality of the risk. It was understood that the CWU (the Communications Workers Union) had continued to challenge the status of agents, proposing that agents should be regarded as workers and a claim had been lodged through ACAS (the Advisory, Conciliation and Arbitration Service). If it progressed there would be some interdependencies with the Group Litigation. The Committee was keen to avoid an implied presumption that the risk to the business model was particular to the status of agents as workers. Project Starling had been established to consider the Taylor Review and wider issues. Its outputs would inform strategic decisions about the evolving business model.

3.5 Subject to the amendments provided, the Committee agreed the proposed changes to the top risks, noted the executive declaration outcomes and confirmed the approach to ARA disclosure as set out in the report for onward submission to the Audit, Risk and Compliance Committee.

DH left the meeting.

4. KEY OPERATIONAL RISKS

Financial Services Conduct Risk Update

4.1 The Financial Services Conduct Risk Update was noted.

4.1.2 AC highlighted the continued risk around out of date branch literature and the importance of demonstrating progress to the ARC. AC queried whether a digital solution was available. JH would review and include an update in future reports.

Change Risk Update

4.2 The Change Risk Update was noted.

4.2.1 JE confirmed that the May ARC report would provide a brief update on the Back Office Transformation and a full update in July. JE would remove Appendix 1, (internal targets for Change management) prior to submission to the ARC.

4.2.2 The Committee was mindful that the ARC had previously requested further detail as to the lessons learned from Change activity over the past three years, and a forward view as to where the principal risks would arise. JH and JE were working with the Chairman to reshape reporting to the ARC from July onwards.

Financial Crime Risk Update

4.3 The Financial Crime Risk Update was noted.

IT Risk and IT Controls Framework Updates

4.4 The IT Risk and IT Controls Framework Updates were noted.

5. INTERNAL AUDIT

Audit Report

5.1 The Internal Audit Report was noted.

5.1.2 The Committee reviewed performance against reporting service level agreements and asked **JA to consider how the reporting and clearance process for IA reports could be streamlined to speed up reporting to the ARC.** At present, there was a challenge in reaching sign off as the reports were initially reviewed by line managers and subsequently, by the relevant GE member(s) prior to Committee. This created a dependency on the availability of key individuals. The Committee suggested that particular thought be given to how report contributors were trained / supported and where GE review was necessary, whether it could be concurrent with line manager review. Turning to recurring control themes and root causes analysis, the Committee suggested an explanation of the remedial action being deployed would be helpful, such as reference to the ongoing control improvement projects. **JA**

5.1.3 It was agreed that the following reports would be provided to the May ARC meeting:

- Back Office Transition (Lessons Learnt)
- SuccessFactors Payroll (Lessons Learnt)
- GDPR Programme
- Project Mercury (Previously Solar HNGT Lite)
- Network Transformation
- Financial Controls Framework.

5.1.4 JA would work with the GE to update the summary of overdue actions prior to the ARC.

6. UPDATES FOR NOTING

DG and JH joined the meeting.

GDPR Programme Update

6.1 DG provided an update on the Post Office programme to achieve compliance with the General Data Protection Regulations ('GDPR') which would come into effect in May 2018. DG reported significant progress since the last programme update resulting in an increased certainty of achieving 'effective' compliance by 25 May 2018 and 'substantive' compliance within the 2018/19 financial year. Contract remediation, however, was a high risk area which remained a potential barrier to achieving effective compliance by the May deadline. The Committee understood that all existing contracts needed to be updated to reflect GDPR requirements. The volume of work represented a significant challenge which had been compounded by a relatively late start to the work.

6.1.2 The contracts work stream had been accelerated with activities for Post Office Management Services Limited and the IT Tower Vendors being prioritised as material contracts. DG drew the Committee's attention to the UK Information Commissioner's statement which provided an indication of the expectation regarding compliance at the May deadline. The Post Office's commitment to compliance, and its role in increasing consumers' trust regarding management of their personal data, would be key considerations should any regulatory scrutiny arise. The Committee noted that a delivery plan would be produced to detail the route to substantive compliance within the current financial year.

6.1.3 A GDPR compliance audit by PwC had highlighted that Post Office was ahead of the marketplace and specifically the financial services benchmark. Responding to questions, DG explained that the complexity of contract remediation had been underestimated resulting in an under-sized resource and a delay to the initiation of the work stream. The Committee observed that a greater understanding of the challenges, following early engagement with the business, would have assisted planning and informed a strategic approach from the outset of the project. The Committee acknowledged that organisational constraints had also had an adverse impact. There had been difficulties in accessing information, gaps in corporate knowledge and a shortage of subject matter skills and competencies. With reference to the programmes management across the organisation, the Committee reflected that an understanding of the scope of each business case and the key dependencies it shared with the overarching programmes would be beneficial.

6.1.4 The Committee noted the report and the material risks to effective compliance identified within, which would continue to be monitored by the GDPR programme steering committee.

6.1.5 The Chairman asked DG to thank the GDPR Programme team for their work to date.

PCI-DSS Compliance Status Update

6.2 JH presented an update on compliance with the Payment Card Industry – Data Security Standards (PCI-DSS). The Committee understood that the Post Office was required to obtain an annual external audit verified attestation on compliance. The existing attestation had expired on 28 December 2017 meaning there was a risk that Global Payments (Post Office's card acquirer) could levy penalties against the Company. Remediation plans had been shared with Global Payments and it was expected that accreditation would be received by 31 July 2018. To date, Global Payments had not taken action.

6.2.1 The Chairman expressed concern that the emerging situation was complex and would require greater understanding to ensure a solution which would not only expedite certification but would also future proof the route to compliance. The Committee was concerned that failure to achieve the verified attestation on compliance by 31 July 2018 could adversely impact the Banking Framework. Accordingly the Chairman would raise the issue at the next GE meeting and a report would be provided to the ARC.

6.2.2 JH advised that Fujitsu was on course to fix all of its items by mid-April but ComputaCenter (CC) (which was now also included within the scope of accreditation) had struggled to complete required actions within an acceptable timeframe. RH suggested that the report to ARC would need to demonstrate a plan of action, referencing the challenges identified together with a list of the avenues explored / exhausted to date. RH would escalate the matter to senior management within CC if needed.

6.2.3 The Committee noted the update on compliance with PCI-DSS.

JH and DG left the meeting.

7. POLICIES FOR APPROVAL

IT Security Policy (Updated)

7.1 The IT Policy had been updated to incorporate all of the additional security standards.

7.1.2 Recognising the policy's links to Change programmes and projects, JE had contacted Hazel Freeman to offer her support.

7.1.3 Responding to questions, the Chairman advised that work to provide assurance against the controls supporting the policy framework would be rolled out during 2018/19. The format of policies had been amended in preparation to include reference the risk(s) they addressed, together with the mitigating control(s) and to identify who was responsible for applying the controls and how frequently they would be applied. JH would be leading an engagement programme to improve understanding across the organisation.

7.1.4 The Committee agreed the changes to the IT Security Policy and recommended the updated policy for onward submission to the ARC.

8. ANY OTHER BUSINESS

8.1 There being no other business, the Chairman closed the meeting at 12.10pm.

....
Chairman

....
Date

Post Office Limited Risk and Compliance Committee
Action List

Status Report as at: 02/07/2018

Meeting Date	AP ref	ACTION	Action Owner	Due Date	STATUS	Open/ Closed
20/07/2017	**1781**	**Insurance Distribution Directive -** Provide a briefing on the potential training requirements of the IDD in order to consider the future compliance burden against capacity in the branch network.	Jonathan Hill	10/07/2018 (July RCC)	Update at March RCC: A plan for initial training on IDD has been written and shared with Post Office Insurance (POMS). A working group would agree the training plan and focus on CPD. JJ advised that he would have a clearer picture of what was needed for implementation in the coming weeks. As POMS was the principal and POL was the appointed representative. Ian Holloway and Jonathan Hill would update on progress at July RCC with a report detailing the requirements, what had been done and what would be done to comply, including timescales.	Open

POST OFFICE
RISK AND COMPLIANCE COMMITTEE

Consolidated Risk Report, including an update on Risk Exceptions

Author: Jenny Elwood Sponsor: Jane Macleod Meeting date: 10 July 2018

Executive Summary

Context

The Post Office Central Risk team has been strengthened by the transferring of the business risk teams from Change, IT, Information Security, Financial Services and Telecoms and Supplier Assurance into the Central team. This change will now enable us to support the business areas to manage risk in a more holistic way, identifying common themes and trends, including risk interdependencies and emerging risks and ultimately improve reporting to RCC and ARC.

This consolidated risk report will continue to evolve over time, as we strive for increased integration of risk MI, insights and trends. As a first step in that journey, this paper brings together previously separate reports. Its purpose is to provide the RCC with the latest version of the Placemat, which now includes results from IT, HR, Communications, Strategy and Identity Services, the current top portfolio risks, where we are with the development of the Strategic Portfolio Office and change delivery improvements, and the current status of Risk Exceptions.

Questions this paper addresses

1. What are the key risks identified from rolling out the placemat in IT, Identity Services, Communications, HR and Strategy?
2. What are the next steps in embedding the placemat approach?
3. What is the current change portfolio delivery status and key delivery challenges?
4. What are the current top portfolio risks and where are we with the development of the Strategic Portfolio Office and change delivery improvements?
5. What is the current status of Risk Exceptions?

Conclusion

1. The Placemat approach has changed the historical, top-down, way of completing risk assessments to a more objective view of top risk alignment. This has given Post Office a deeper understanding of its risk profile.

2. Through engagement in workshops with over 70 teams, the implementation has encouraged a dialogue around the operational risks by business area and has prioritised remedial activity to reduce the impact of the highest risks.

3. The final roll-out of the Placemat to the areas of IT, Identity Services, Communications, HR, and Strategy has taken place. A full update is shown in paragraphs 10- 15. For IT the rollout provided affirmation that the top risks identified through their existing risk process remained the same, for Identity Services discussions were around their early thoughts on their strategy so as the proposition progresses the risk landscape could change.

This roll out has not identified any risks which change the current Top Risk's agreed at May's ARC.

4. Our aim is to develop further our risk management maturity and the Placemat process to further embed a more mature risk culture and enhance risk oversight and reporting, improve awareness, controls and assist in identifying business priorities. Next key steps include:
   - quarterly placemat refresh to improve the completeness and quality of risk and control information;
   - identify and work through the strategic risks for Post Office;
   - equip and enable the business to manage/report their operational risks;
   - enhance the risk exceptions process; and,
   - construct a dashboard which represents the key principal risks (referred to as 'horizontals') to provide improved insight to Executives and SteerCo's and further embed risk framework governance, oversight and reporting.

5. The next scheduled full Placemat re-assessment will be brought back to ARC in September.

6. The top portfolio risks remain i) Risk of increased costs and delayed benefits through late delivery of Change and ii) EUM effectiveness. These are relatively stable and mitigation work continues. The development of the Strategic Portfolio Office and improvements in change delivery continues at pace. A full update is provided in paragraphs 17 to 24.

7. There are 9 live Risk Exceptions for noting, shown in appendix 3.

Input Sought

8. The Committee is asked to review and comment on the report.

The Report

What are the key risks identified from rolling out the placemat in IT, Identity Services, Communications, HR, and Strategy?

IT

10. During quarter 1 we introduced the placemat to IT. There are 51 risks in total, including 11 high risks and 3 top risks. The reassessment of risk has resulted in a 15% reduction in the number of high risks compared to the previous quarter. This is the result of better processes and controls, most notably due to the completion of the Horizon Datacentre refresh programme and ensuring that our key admin and cash centres have primary and secondary connections available to reduce service interruption. The 3 top risks are detailed below, with further improvements expected over the next 4 months:

- **POLSAP** - is the remaining highest risk system and will be until Sept / Oct (dependent on delivery progress), when Cash Processing (already live in Belfast) is planned to migrate all other cash centres onto a new system, and our financial and sales processes are re-modelled and deployed onto CFS (our more modern ERP):

Risk Title	Risk	Current RAG	Mitigation Plan	Due date	Target RAG
POLSAP Legacy Systems	Failure to ensure all components are fully supported by the appropriate levels of adequate technology, hardware, whilst programme activities are in progress, may lead to a loss of service within Supply Chain and Finance Teams, resulting in service unavailability, financial loss, reputational damage and Security Vulnerabilities.	**20** **I/L** **5:4**	a) POLSAP Processes migrated to core finance. b) Migrate cash processing off POLSAP to Transtrack CWC, already live in Belfast. c) POLSAP Hosting Contract Extension – period April 1st to December 31st 2018. d) FJ Network Upgrade complete, removing security risk of old switches (reducing the likelihood of security incidents) e) POLSAP spares being reviewed monthly, currently remaining within tolerance.	a) 25.09.18 b) 25.09.18 c) 31.12.18 d) Complete e) Ongoing	**6** **I/L** **3:2**

- **Fujitsu Failover Horizon Datacentre Failover Test –** The decommissioning of POLSAP from Fujitsu is scheduled to take place in September 2018. It is recommended by Post Office IT and Fujitsu that we carry out a full recovery exercise at a suitable Bank holiday weekend in Spring 2019, as this will give contingency in the event of any issues being encountered, following the earlier decommission:

Risk Title	Risk	Current RAG	Mitigation Plan	Due date	Target RAG
Horizon Datacentre Failover Test	Failure by Post Office IT to ensure that a full Disaster recovery test is carried out on a regular basis in line with contractual agreements, may lead to being unable to restore primary servers and services not being restored in a real outage. Resulting in financial losses, reputational damage, and prolonged service interruption.	**20** **I/L** **5:4**	a) Ensure that all planned tests that Fujitsu have agreed are implemented over the next 11 months. b) Branch Database failover scheduled for the 31st August 2018. c) Failover test scheduled Easter 2019.	a) 31.12.18 b) 07.09.18 c) 26.04.19 d) Ongoing	**6** **I/L** **3:2**

Risk Title	Risk	Current RAG	Mitigation Plan	Due date	Target RAG
			d) Monthly IT Service Continuity reviews in place.		

- **PCI Compliance** – Post Office are without a Report on Compliance (RoC) from external qualified security assessors (QSA) proving our compliance to the Payment Card Industry – Data Security Standard (PCI-DSS). However, we believe that our environment has no Data or IT security exposures. We are continuing to work closely with our stakeholders, ensuring they have visibility of our remediation plan. Both the Acquiring bank and Qualified Security Assessor (QSA) are comfortable we are addressing the risk of non-compliance and a Steering Group has been set up to oversee the remediation work, explore more strategic solutions and will continually re-assess this risk:

Risk Title	Risk	Current RAG	Mitigation Plan	Due date	Target RAG
PCI Compliance	The 2017 PCI Audit identified a number of Audit Actions across IT 3rd party suppliers which are "not yet compliant". Failure by Post Office to address these findings and provide a robust plan to resolve these actions within an estimated timescale of 12 – 24 months, may result in challenges during external audits, require remediation activities and attract unbudgeted remediation costs. Ultimate penalties could result from Post Office failure to not evidence a plan of works towards compliance e.g. failure to obtain the required certification and reduce our ability to develop our strategy where it requires us to be fully PCIDSS complaint.	12 I/L 4:3	a) Conclude audits and work through the current identified actions for FJ and CC All scheduled to complete end of October 2018 b) Initiate a Programme to scope PCI compliance strategy (Project Manager / Co-ordinator) and run within IT4IT with Service Operations sponsoring c) Plan for 2018 audit scope d) Set up a business engaged e) Introduce compensating controls on any non-compliances that will not be closed by 31st July and work with QSA / Acquiring bank. f) QSA states that we are not at immediate risk of penalties or sanctions and this will be continually reassessed	a) 31.10.18 b) In progress c) In progress d) 05.07.2018 e) 31.07.18 f) On-going	6 I/L 3:2

Identity Services

11. For Identity Services, the risks are reflective of the developing stage for their business. 10 risks have been identified with the top 3 amber risks being:

Risk Title	Risk	Current RAG	Mitigation Plan
Supplier Risk	The risk of inadequate and/or ineffective procedures to select and manage technology suppliers. This could result in slowing down product development and services, leading to loss of market share	9 I/L 3:3	a) Key person risk and lack of flexibility with suppliers; b) Capability of the supplier to deliver requirements; and c) Strategic and operational alignment with suppliers.
Market proposition including product and competitive-ness risk	The risk to Identity Services' ability to exact a product offering to meet the needs of the customer, and keeping pace with the market to remain competitive	8 I/L 4:2	The Identity proposition is currently being worked through, and once developed it may have an impact on the risk profile. In the meantime, the following mitigations are being progressed: a) An agile strategic business model which can respond to emerging markets and new entrants, by reducing the time to deliver new processes and technological changes; b) The attractiveness and relevance of the product and services proposition, to meet the customer and market expectations; and c) The ability to maintain a market leading competitive advantage and to support continued sponsorship of Government products and services.
Data Protection	The risk of development and launch of sub-standard products	8	a) Design of product will be in line with industry required DP and IT standards

and Information Security	with inadequate DP and IT security. This may result in regulatory action and/or adverse media coverage leading to financial and potential reputational loss	I/L 4:2	b) Appropriate pen and security testing will be undertaken

Communications

12. Communications have identified 13 risks, with the following top red risk:

Risk Title	Risk	Current RAG	Mitigation Plan
Fragmentation of relationships with UKGI impacting effective communications and working methods	There is a risk that working relationships with UKGI become more fragmented, as a new teams beds in and roles are clarified, leading to less effective delivery of our business and governance strategies. Wholesale staff changes at UKGI seem to be resulting in multiple approaches o colleagues across the business, with previous practice of a more centrally co-ordinated system of information flow coming under some strain. A potential policy sponsorship role within BEIS itself is a welcome development, but will make the need for effective coordination more pronounced.	12 I/L 4:3	We are developing a framework document with UKGI, which ought to set out the roles, responsibilities, communication, and reporting requirements more clearly. In addition, the corporate affairs team continues to work with UKGI to develop greater understanding of the two organisations' needs through, e.g., joint team workshops, the second of which is planned for later this month.

Human Resources

13. HR have identified 54 risks with the following 5 top risks:

Risk Title	Risk	Current RAG	Mitigation Plan
Industrial relations	There remains a risk of industrial action as a result of Pay, CDC Pensions, DMB strategy and/ or a conflation of these.	16 I/L 4:4	Significant work has been done to mitigate the impact including dialogues with stakeholders, national collective engagement framework and contingency planning. Previous industrial actions have resulted in minimal disruption of service to our customers and did not receive any significant media coverage.
Digital competency	There is an ever increasing reliance on, and demands of, services through the digital medium. The Post Office strategy is to continue to enhance its digital offering as part of its 'North Star' strategy. Failure to attract, retain and develop appropriate competence would adversely affect the growth strategy and business model and could result in financial and reputational loss and regulatory sanctions.	12 I/L 3:4	a) Working with CIO to identify additional channels to attract talent b) Digital workplace programme established c) Digital workplace lead and Office 365 trainer to be hired d) SuccessFactors e-learning in place e) Digital Stars network being established f) Investment in Business Innovation Centre (101 Finsbury Pavement)
Key person dependency	There is a significant amount of business knowledge and experience covered by a few key individuals. This key person dependency is a risk to our North Star strategy which will be impacted significantly if these key individuals suddenly left the business	12 I/L 4:3	a) Quarterly meetings in place with GE members and their direct reports to discuss succession plans, 'flight' risks and high potential team members b) New handover process c) Training and development needs identified for talent.
Breach of employment regulation and legislation	Breach of employment regulation and legislation is an increasing risk due to the increasing legislation, and in light of recent judgements	8 I/L 4:2	a) The Post Office has been managing this risk through policies, companywide communications, engagement strategy and periodic training.
Agency status	There is a risk that undetermined status of Agents could result in regulatory intervention which could have a significant impact on the sustainability of our business model.	10 I/L 5:2	a) Developments in case law related to this are being closely monitored

Strategy

14. The risks identified by the Strategy team relate to delivery of their responsibilities, as oppose to the strategic risks to the Post Office. The latter will be addressed through the Central Risk team work (see paragraph 16). The Strategy team has identified one key amber risk relating to dependence on key personnel. Plans are in place to use interns to capture the knowledge to ensure continuity and minimise the impact of the sudden departure of key personnel. This risk is reported through the wider HR key person dependency risk.

15. Please refer to Appendix 1 for the completed Placemat. Please note that during the period being reported upon, the focus has been on rolling-out the placemat to the five remaining business areas. The risk position for other business areas (Retail, FS&T, LRG and F&O) remains the same as was reported in March 2018.

What are the next steps in embedding the placemat approach?

16. Our aim is to improve our risk management maturity to support the delivery of North Star ambitions and strategic priorities, while keeping the business compliant, resilient and sustainable. Appendix 2 provides our assessment of where we are now and where we aspire to be. The next phase of the Placemat roll-out will further embed the risk framework to enable enhanced risk oversight and reporting, through:
    - quarterly placemat refresh to improve the completeness and quality of risk and control information. This will include risk and control descriptions, scoring rationale and consistency, principal risk consolidation and linking through the connected events to support the view, such as Audit findings and incidents;
    - identifying, assessing and managing strategic risks to Post Office achieving its North Star ambitions and delivering on its strategic priorities;
    - Develop executive reporting and oversight perspective on the 'top risks'. Reviewing more closely those risks which, if not monitored and managed, could create harm to the Post Office and its strategic objectives;
    - simplifying the risk exceptions process and exploring ways to digitise it providing greater effectiveness and efficiency in raising and subsequently approving, monitoring and reporting of exceptions; and
    - constructing a dashboard for the key principal risks currently being piloted for Financial Crime, Safety and Information Security. The dashboard will provide a view of how Post Office is performing against the relevant principal risks pulling together performance and risks MI (including results of any recent assurance/audit work) enabling us to track risk performance and where we are against risk appetite.

What is the current change portfolio delivery status and key delivery challenges?

10. In June 2018 the HNGT Lite business case was reporting red from a delivery perspective due to unallocated Cloud Enablement costs causing the

financial position to be in exception. Since then the costs have been correctly allocated and the financial position updated. The programme delivered a functioning pilot to the June Board and is on track to deliver the first Live Retailer POS-integrated pilot sites in August. The programme is reporting Amber whilst a PCI issue is resolved in the underlying infrastructure. This has the potential to push the date out but the current position is that the impact should be limited to one week's slippage.

11. The capability delivered by HNGT Lite programme is being taken forward into a new business case later in July.

12. Back Office Transformation has amended its go live date to September 2018 and is reporting Amber. Challenges remain as there is little contingency. At this point the programme is around 45% through its second integration test cycle with a 78% pass rate. This is slightly behind plan. High volume validation of settlement and billing calculations against historical data are in progress and are matching expected results for the POLSAP Migration Project, but issues have been found with process & technical system performance which are being worked through. A 3rd party has been engaged to review test coverage and provide a report on suitability. The challenges of completing the build and testing of the cash processing project remain. Mitigations have been implemented. The residual risk is that cash processing plans are tight.

13. Key achievements secured since the last ARC include:
    - Customer Hub: The Post Office Travel App went live in June 2018 with some low risk activities outstanding. As full update is provided in the separate Compliance report.
    - General Data Protection Regulations (GDPR): GDPR came into force in May 2018. Through adopting a risk-based approach, we have essentially secured 'effective compliance' with the requirements of the new legislation, although we did not reach the desired level of contract remediation. Work continues to improve the position on material contracts by end of July. A full update on reaching 'substantive compliance' is provided in the Compliance report.

What are the current top portfolio risks and where are we with the development of the Strategic Portfolio Office and change delivery improvements?

14. The current portfolio top risks remain i) Risk of increased costs and delayed benefits through the late delivery of Change and ii) EUM effectiveness.

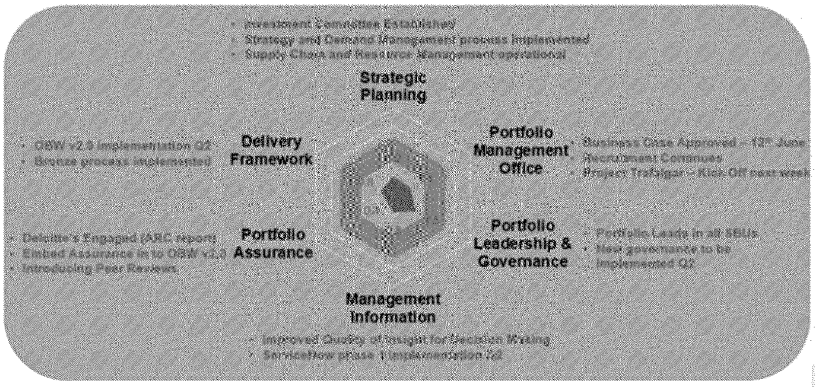
15. In terms of the overall portfolio we currently have **18** active change portfolio risks but the Change Risk & Assurance team are currently undertaking a comprehensive review to ensure they remain consistent with the change challenges currently facing the Post Office. This work will be completed by end July 2018 at which point the portfolio risks will be re-baselined. The output of this work will be provided to ARC in Sept 2018.

Late delivery of change and an update on the Strategic Portfolio Office

16. In November 2017, the GE endorsed analysis which concluded that due to systemic problems the current change capability was not mature enough to deliver the strategic outcomes of the business and recommended changes to structure, governance, culture and competency to address these issues. They approved a £500k seed investment for the Assess phase.

17. In January 2018, PA Consulting undertook a maturity assessment of the current capability against other organisations operating in the retail and financial services market. PA rated Post Office at 1,[1] out of 5, compared with an average score of 3.5 and 4 respectively. Since then a high-level design for a new change target operating model (TOM) has been developed and work is now underway to implement this so that we can address the fundamental issues and attain the necessary maturity levels required to fulfil our strategic goals.

18. A key objective of implementing this TOM will be to increase the maturity from 1 to 3 within 12 months (around June 2019), to mitigate the systemic issues identified and to establish the foundations for continuous improvement thereafter. An update on the activities to drive up the capability maturity model is shown below.



Strategic Planning
- Investment Committee Established
- Strategy and Demand Management process implemented
- Supply Chain and Resource Management operational

Portfolio Management Office
- Business Case Approved – 12th June
- Recruitment Continues
- Project Trafalgar – Kick Off next week

Portfolio Leadership & Governance
- Portfolio Leads in all SBUs
- New governance to be implemented Q2

Management Information
- Improved Quality of Insight for Decision Making
- ServiceNow phase 1 implementation Q2

Portfolio Assurance
- Deloitte's Engaged (ARC report)
- Embed Assurance in to OBW v2.0
- Introducing Peer Reviews

Delivery Framework
- OBW v2.0 implementation Q2
- Bronze process implemented

19. A more focused Investment Committee is in place and a new UKGI quarterly reporting framework and the establishment of a new Strategic Portfolio Office.

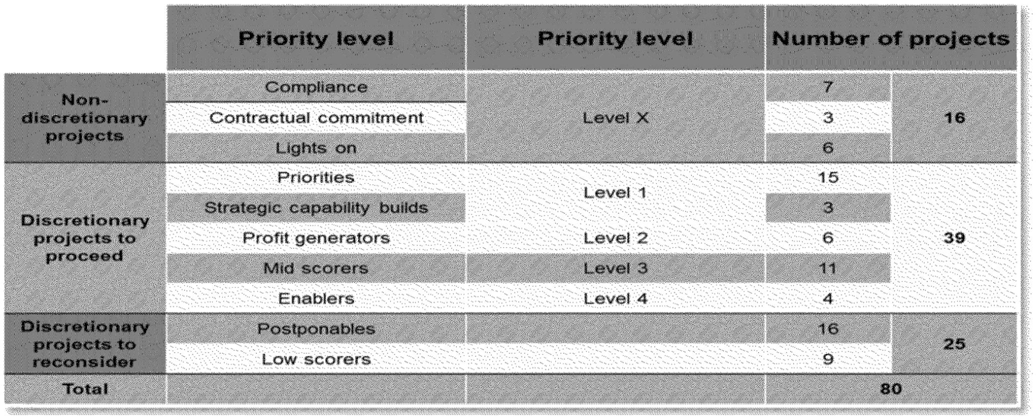
20. Following Investment Committee approval of the Business Case in June 2018 work is underway on the delivery of Phase 1. This is targeted for completion by September 2018. Key deliverables in this phase include:
    - a full Agile Business Case and an implementation roadmap;

[1] Capability Maturity Model Integration (CMMI) Level 1 (Initial) –whilst processes exist they are not always fit for purpose, nor are they consistently applied or adequately governed and consequently the organisation is often reactive in its management.
CMMI Level 4 (Quantitatively Managed) – This builds on level 3 practices and uses statistical and other quantitative techniques to understand performance variation. It identifies and understands variation, and predicts and improves the ability to achieve quality and process performance objectives.
CMMI Level 5 (Optimizing) – This builds on level 4 practices and uses statistical and other quantitative techniques to optimize performance and improvement to achieve quality and process performance objectives.
In practice it is expected that the Post Office will probably achieve 4 in some dimensions and only 2 in others thereby achieving an overall average of 3.

- detailed funding plan for Phase 2;
- development of a Post Office Scaled Agile Framework (SAFe)[2]; and,
- continued implementation of quick-wins including the recruitment of key roles into Strategic Portfolio Office.

21. Phase 1 also includes the development of a prioritised Investment Portfolio for 2018/19, the introduction of One Best Way improvements and enhancements to governance. This includes replacing the existing Change Approvals Group with Change and Portfolio Performance Review Committees to provide better focus.

22. The SPO is undertaking a prioritisation and optimisation exercise on the change portfolio. This involves an assessment of the pipeline of future programme and projects against set criteria to ensure we focus on delivering those Change initiatives which deliver the North Star and financial goals whilst generating the optimal returns on investment within an acceptable risk envelope. This has been initially assessed by the portfolio managers of the respective business units and then subject to peer review. This work being reviewed and managed at the Investment Committee but is summarised in the following table.



	Priority level	Priority level	Number of projects	
Non-discretionary projects	Compliance	Level X	7	16
	Contractual commitment		3	
	Lights on		6	
Discretionary projects to proceed	Priorities	Level 1	15	39
	Strategic capability builds		3	
	Profit generators	Level 2	6	
	Mid scorers	Level 3	11	
	Enablers	Level 4	4	
Discretionary projects to reconsider	Postponables		16	25
	Low scorers		9	
Total			80	

23. Work has also been initiated on integrating risk & assurance lessons learned into core processes and building a Competency Assessment and Development Plan for the wider change community. Deloitte have been briefed on the TOM to ensure the appropriate controls and assurance are being implemented to address the lessons learned. We await a copy of their report and recommendations.

24. Finally, we have also recently commissioned Deloitte to undertake some separate work on the emerging change assurance model to provide

[2] SAFe is the leading industry framework for implementing Scaled Agile and will be tailored to meet the specific needs of the Post Office.

additional assurance that the way forward, and progress against it, is sufficiently comprehensive and robust.

Risk Title	Risk	Current RAG	Mitigation Plan	Due date	Target RAG
Late Delivery of Change	Our change is delivered late, risking costs and benefits or has unintended consequence	15 I/L: 3:5	• Phased Transition plan: phase 1 developed and actively being tracked, stories are being implemented using an agile methodology. Objective is to treble maturity in 12 months.	31/7	6 I/L: 2:3
			• Project prioritisation: Ideation collection and prioritisation process developed. Initial prioritised project list shared at Investment committee on 23/4	31/7	
			• Investment committee: in place, ways of working will develop and be improved as Investment Committee and support forums mature.	Complete	
			• Strategic portfolio office:		
			○ launched	Complete	
			○ recruitment completed	30/9	
			○ target operating model phase 1	30/9	
			○ target operating model phase 2	31/3/19	

Enhanced User Management (EUM)

25. The EUM delivery plan is progressing well. As at 25 June, the Programme had rolled out the new identity solution to 3,885 branches (an increase of over 1,400 branches since the last ARC submission) and is on target to achieve over 6,000 branches by end of July. This equates to 20,000 individual users in our largest branches covering over 90% of POMS sales. We are also seeing improved training compliance for Smart ID branches at 89% for individuals. Unfortunately, it is not possible to directly compare to non-Smart ID branches as individual performance data is not gathered.

26. The collection and cleansing of agent and agent assistant data is still a key dependency for EUM. Based on current response levels, we estimate a non-conforming tail of around 1,900 branches by the end of the programme. A tail management plan is underway to address this, including issuing a single Smart ID to the branch owner and disabling all other Horizon IDs. This would following an intensive period of chasing, including branch visits to minimise the numbers of branches impacted.

27. The programme is still planning full roll-out by November 2018 and deployment of training controls to commence in October 2018 and complete by January 2019.

28. To support this transition the programme have completed the design of a structured set of measureable go/no-go criteria around switching on the training controls beginning in October 2018. A GE update is planned for August 2018 so that the risk profile of implementing training controls for the first group of branches is understood and agreed before the programme takes action.

Risk Title	Risk	Current RAG	Mitigation Plan	Due date	Target RAG
EUM	There is a risk that EUM does not perform as expected due to • being unable to collate accurate data from agents • POL staff/agents not having an individual email address	12 I/L: 4:3	• Branch Standards: Uplifted team in place although recruiting continues for final 2 FTE resource. New Branch Standards Team Supervisor in place to manage the new FTEs, share	Complete	9 I/L: 3:3

Risk Title	Risk	Current RAG	Mitigation Plan	Due date	Target RAG
	which can be used to communicate logins and training information **(resolved)** • Agents not being able to access SuccessFactors via the internet/browser solution **(resolved in new design)** This all leads to our inability to address the key business goal, which is for POL to prove to its client that persons transacting on its behalf are suitably qualified and vetted.	■	knowledge and manage escalations. • Horizon/LMS interface: to ensure continuity/integrity of training data is in build. Technical integration is now live, with final Horizon changes being implemented as part of Release at end of July 2018. • EUM: Escalation plan implemented by Common Services team to chase branches data capture, this includes dedicated NBSC team calling branches. EUM currently is currently on track to be live in over 6000 branches by end of July 18.	12 July 30/7	▨

What is the current status of Risk Exceptions?

29. There are 9 current approved Risk Exceptions for noting.
    - 7 new Risk Exception Requests (RER) were approved since the last report. Of these, 4 relate to the Customer Hub;
    - 1 RER relating to Robotics was closed; and
    - 3 RERs relating to SalesForce, SuccessFactors and Call Centre Recording have overdue action(s).

30. The details of the existing and new Risk Exception Notes can be found in Appendix 3.

31. As mentioned in paragraph 16 above, the Central Risk team are also simplifying the risk exceptions process and exploring ways to digitise it to enable greater effectiveness and efficiency in identifying, analysis, reviewing, approving, monitoring and reporting of risk exceptions.

Appendix 1: Placemat

To follow

Appendix 2: Embedding Placemat – Current Maturity and Forward Plan

We have assessed the maturity of our risk management framework against observed good practices using Deloitte's maturity model. The table below outlines our assessment against the different attributes in terms of where we are today (at the end of FY17-18) and what activities supported this; our target for FY18-19 and what interventions we propose to make; and our aspiration for FY19-20 and beyond. These take into consideratioin the benefits that each stage of maturity provide to the organistion.

We believe that our plans will allow us to realise benefits from risk management in the pursuit of our North Star Ambitions and build confidence in the delivery of our strategic priorities, but also help us to align with the principles that underpin the spirit of the UK Corporate Governance Code in a proportionate manner.

	Objective	What	Examples	FY17-18 Assessment (and enabling initiatives delivered)		FY18-19 Target (and enabling initiatives proposed)		FY19-20+ Aspiration
Driving Shareholder Value Guarding the Balance Sheet – Protecting the Brand	License to Operate	Meeting legal, regulatory and social obligations	• Good Governance • Compliance with Laws and Regulation	◕	• Effective Board and GE level governance through ARC and RCC • Strong focus on complying with all laws and regulations	●	• Strengthening governance over principals risks using pilots in Financial Crime, Safety and Information protection • Prioritised focus on remediating gaps to be compliant (eg PCI, GDPR) through collaborating of compliance and risk team	●
	Protecting Value	Minimising loss and protecting shareholder value, brand and reputation	• Control Frameworks • Third Party Risk Management • Business Continuity • Board Approved Policies	◑	• IT and Financial Controls frameworks implemented • Board approved policies in place in several areas • Business Continuity assessment commenced	◕	• Assurance over departmental effectiveness of controls assessment (IT and Finance) • Assurance over minimum controls within policies • Increased focus on supplier risk assurance	●
	Driving Efficiency	Doing Things Right Business Efficiency	• Understanding Complete Risk Profile • Consistent Processes • Prioritising Remediation	◑	• Placemat 1 rolled-out to develop bottom-up risk profile • Focus on risk identification and assessment	◕	• Placemat 2 to focus on driving consistency and prioritising remediation of top-risks • Focus on managing risks through effective and operational controls • Consolidated Risk Reporting to join the dots across risk types/ sources to provide insights/trends (enterprise, change, IT)	●
	Creating Value	Doing the Right Things Where and When to take a 'Risk'	• Better Decision Making • Strategic Risk Appetite • Embedded Risk Culture	◔	• Limited consideration of risks in key business decisions • Board approved appetite statements but not refreshed or applied • Risk Exceptions process in place but not applied consistently or timely • Varying levels of business engagement	◑	• Risks assessed proactively for key initiatives (eg CHUB, Identity etc) • Making risk appetite real through use of leading and lagging indicators, and monitoring progress • Simplifying and digitising risk exception process • Encouraging, equipping and enabling businesses to manage and report on their operational risks	◕

	Adhoc ◔	Fragmented ◑	Coordinated ◕	Integrated ●	Intelligent ●
Benefits and Challenges	× Operational and financial surprises are pervasive × Operate in the belief that everyone will always do the right thing × Management bandwidth consumed by issue management	✓ Issues begin to surface rather than being ignored or hidden × Focus on symptoms rather than root causes × Absence of learning environment resulting in repeat incidents	✓ Holistic view of key risks facing the organisation from both internal and external environment ✓ Enables more proactive mitigation of risks through controls, ✓ Fewer repeat incidents as root causes addressed	✓ Clarity on accountabilities and decision rights ✓ Stakeholder confidence through 'joined-up' view on efficacy and proportionality of the controls environment ✓ Operational efficiency gains through an optimised risk operating model ✓ Risk management and performance management are separate conversations	✓ Risk management is embedded in performance management ✓ Agility in anticipating and responding to issues ✓ Ability to exploit uncertainty to drive value
UK Corporate Governance Code				▲	

Appendix 3: Risk Exceptions

Title (Type) and Risk	Owner	Date	Actions	Due Date	Status/ Update
SalesForce – Procurement (Regulatory) Contract has been renewed / extended non-compliantly for a period of 12 months.	GE-Owen Woodley Accountable-Chrysanthy Pispinis	Raised: 21-Apr-17	POL should seek to run a full compliant procurement as soon as possible to reduce the risk of a challenge.	29-Apr-18	**Overdue.** - We intend to award a new compliant contract to Salesforce under the Software Reseller Framework, recently awarded to Specialist Computer Centres Plc ("SCC"). This is more cost-effective and flexible than previously identified via CDP and Accenture. The Salesforce contract expired on 29th April 2018. To finalise negotiations, Salesforce have since executed two 30-day extensions, the 2nd of which expires on 29th June 2018. The PO and Salesforce legal teams are currently finalising contracts
Success Factors (Regulatory) Implementation of Success Factors without addressing certain data protection and information security risks could result in breach of data protection regulation and Post Office policy requirements as line managers can download, copy, export and distribute, personal data of their team members, via non-corporate devices.	GE-Martin Kirke Accountable-Martyn Lewis	Raised: 02-Jan-18	Directive from Group HR Director for declaration to be signed by the staff in HR Service Centre	08-Jan-18	**Closed**.
			Weekly report to monitor access via IP addresses of non-corporate devices	08-Jan-2018	**Closed–** No longer required due to action 3.
			Installation of a password manager	26-Jan-18	**Closed.**
			Suitable training and information during the roll out of SuccessFactors (SF) to all line managers and new joiners.	08-Jan-18	Measures to be put in place: - **Closed.** - **On-going, to be included in the 18/19 compliance test.** Compliance training Info Sec/DP, updated module content to reflect.
			A corporate solution (combination of SSO/BYOD)	30-Jun-18	**On-going/ will not be completed on time. Exception will be renewed in July 2018.** • An effective temporary solution was introduced limiting all those with wide access to employee data to accessing only from their work machines. This covers all HRSC staff, will remain in place until SSO provides the restriction. • Wide access to employee data is controlled by SF roles • SSO is a part of the JML project which received funding approval last month, the team has now been mobilized. SSO for SF will be deployed first, plans indicate by Mid-July. • BYOD has been rolled out for all phones for email, but it does not cover SF, nor does it cover external laptops (planned to be rolled out over the next couple of months). • SSO & BYOD as described above will not adhere to the purpose outlined above. A 2nd stage to the JML project is to deploy rulesets for groups to limit access to our network. The HRSC team / other users who require wide personal access to data, will be placed into a group that limits access to SF on our network. The temporary solution will remain in place until such time. • Design discussions are occurring on whether BYOD (inTune) can be extended to control SF access when partnered with SSO/MIM. In the case this is possible the control will be extended. • A control is now in TrAction – to confirm monthly that access has not been granted to any user who is not technical limited to our network. Recommendation is either A) that we close this reporting point due to the preventative & reactive controls already in place, or B) report back again in 4-6 months on situation with a view to close at that time.
Contact Centre Call Recording data storage in EEA (Regulatory) Data storage at rest is not compliant with Post Office's Government contracts - There is a very small risk that personal data relating to Government	GE-Al Cameron Accountable-Gayle Peacock	Raised: 04-May-18	All call recordings will be encrypted at rest	15-May-18	**Overdue.** Will be implemented when the new solution will be delivered by Verizon. Implementation date awaited.
			Call recordings will be stored for no longer than needful.	15-May-18	
			No identifiable personal data for government clients to be collected	15-May-18	

services would be included in call recordings. - The recordings will be encrypted and held securely in Oslo.			Any changes to the status of data held in the EEA to be monitored	On-going	
			Obtain permission from clients linked to the FOCS contract to retain call recordings dealing primarily with transactional (non-personal) data off-shore within the EEA.	04-Nov-18	**Not yet due.**
Deferred Checking Pilot (Risk Appetite) Pilot relies on a physical mandate being held by PO branches and checked whenever a TimeSaver customer uses the service, potentially exposing PO to financial crime, fraud or financial loss.	GE-Debbie Smith Accountable-Greg Lewis	Raised: 01-Mar-18	As a preventative control clear branch communications will be sent out to the Post Office branches using TimeSaver together with the customer indemnities for their branch. As the service is rolled out further additional branch focus articles will be written. Clear instructions will also be detailed on the pouches advising branches not to hand out to customers who are not signed up to the TimeSaver service. For this pilot, the manual mandate process is the only option, but Post Office is looking at what technical solutions could be available that will enable an 'online' check of the mandate at point of sale.	31/07/2018	**Not yet due.** **Completed.** The workshop has taken place. To progress further engagement with ATOS is required to understand and cost options and progress if deemed worthwhile under a separate business case.
			As a preventative control participating Banks are only offering the TimeSaver service to established customers, not all customers (as this reduces their risk and liability under the indemnity to Post Office). The banks will assess the suitability of their customer for the service.		**Completed.** This is embedded in the service offering.
			The product team will monitor branch discrepancies and escalate any significant issues for further investigation to the Financial Crime Team	Weekly from 17/5/18	**Completed.** This is embedded in the service offering. No discrepancies have taken place in the pilot to date.
			TimeSaver is designed to allow efficient queue management, and to speed up the deposit process rather than increase the level of cash over Post Office counters. Increase in cash levels is being considered as part of the Future of Cash Business Case.	Business case being presented to Board on 16/5/18	**Completed.** No action required within pilot.
			Additionally, the pilot will be evaluated before the service is rolled out further. Feedback will be sought from branches who have customers using the service	Evaluation from July 2018	**Not yet due.** The pilot has not yet completed its 8 week duration
Customer Hub - Accessibility (Policy) The Customer Hub app does not currently conform to WCAG 2.0 or an agreed set of Cust Hub accessibility requirements yet. This could risk a customer mounting a legal challenge against the Post Office for not making the app accessible enough or meeting WCAG compliance to level AA.	GE-Owen Woodley Accountable- Hose Carbajo	Raised: 01-Jun-18	Hub will target WCAG compliance following IDD travel insurance changes being implemented for Sept 2018, as implementing in advance will incur significant rework and cost.	31-Dec-18	**Not yet due.**
Customer Hub - Encryption (Policy) The Customer Hub app and the back end system use varying encryption techniques which are incompatible.	GE-Owen Woodley Accountable-Ray	Raise: 01-Jun-	As part of the migration of CDP from UKCloud to the new infrastructure provider, a new full encryption service will be provisioned. This will provide the ability to use 'convergent encryption' and thus email and phone number fields can be encrypted and encryption will be performed in	31-Oct-18	**Not yet due.**

POL00401627

It's not possible to encrypt the email address /phone number data items since these are the critical fields needed for the search.			equivalent of the Hashicorp vault service. Unless the approach / architecture of storing Customer details changes, the Hub will mitigate the risk as part of the CDP transition timescales		
Customer Hub - Twilio Contract (Regulatory) The Twilio MSA will not be signed by the launch date of 11 June. Twilio services can be used in advance of MSA being agreed, but doing so means using service under Twilio's standard t&cs and will need funding by credit card on the account.	GE-Owen Woodley Accountable- Francisco Pazo Couto	Raised: 05-Jun-18	Contract to be signed by 30 June 2018	30-Jun-18	**Closed.**
Customer Hub - FRES Contract (Regulatory) PO is in process of negotiating a side letter to the Travel Money Card Arrangements agreement between POL, FRES and FISA Payments. FIS have not been involved in the negotiations to date and will be asked to consider the terms of the side letter once POL and have FRES have reached agreement. The agreement is not binding without FIS's approval, and as this is a tripartite agreement this poses a significant risk to POL in that FIS may reject or wish to renegotiate terms	GE-Owen Woodley Accountable- Francisco Pazo Couto	Raised: 30-May-18	An email will be sent to BOI UK and FRES (the JVCo) for them to confirm the ownership of the API and the process to be followed should FRES wish to leverage the technology and licence separately in the future.	31-May-18	**Closed.**
			The contract negotiations are near completion. POL is aiming to conclude negotiations with FRES by 8th June, and it is expected that FIS review will be completed by 15th June.	15-Jun-18	**Closed.**
			FRES will obtain the approval of its board of directors and shareholders to its accepting and implementing the terms of the side letter.	30-Jun-18	**In-progress.** The request to approve the Letter has been sent to BoI's shareholder representative, following which it will be countersigned by the authorised signatories of FRES and BoI. POL's shareholder representative has formally approved the Letter.
Lawyers on Demand (Regulatory) The Legal Team has no capacity to deal with Peregrine and Cust Hub. The decision was made and approved by the project owners that external legal support should be brought in to support the 2 projects. The Legal Team engaged with other external providers and legal firms. None of them was able to provide a candidate that is suitable for this role with the relevant experience. Due to the stringent deadlines, it was not viable to run a public procurement process to appoint LOD as a service provider. This risk exception was to approve the Legal Team to engage with LOD and on-board them as a supplier without going through the public procurement process.	GE-Owen Woodley Accountable- Francisco Pazo Couto	Raised: June 2018	There is no mitigation. The resource will be in place until such time that the two projects do not require legal expertise	N/A	**N/A**

POST OFFICE
RISK AND COMPLIANCE COMMITTEE

PAGE 1 OF 8
NOTING PAPER

Internal Audit Report

Author: Johann Appel   Sponsor: Jane MacLeod   Meeting date: 10 July 2018

Executive Summary

Context

The purpose of this paper is to update the Committee on the PO Internal Audit activity and key outcomes. This includes details of the work completed since the last Risk and Compliance Committee (RCC) and Audit, Risk and Compliance Committee (ARC) meetings in May and progress on delivery of the Internal Audit Plan.

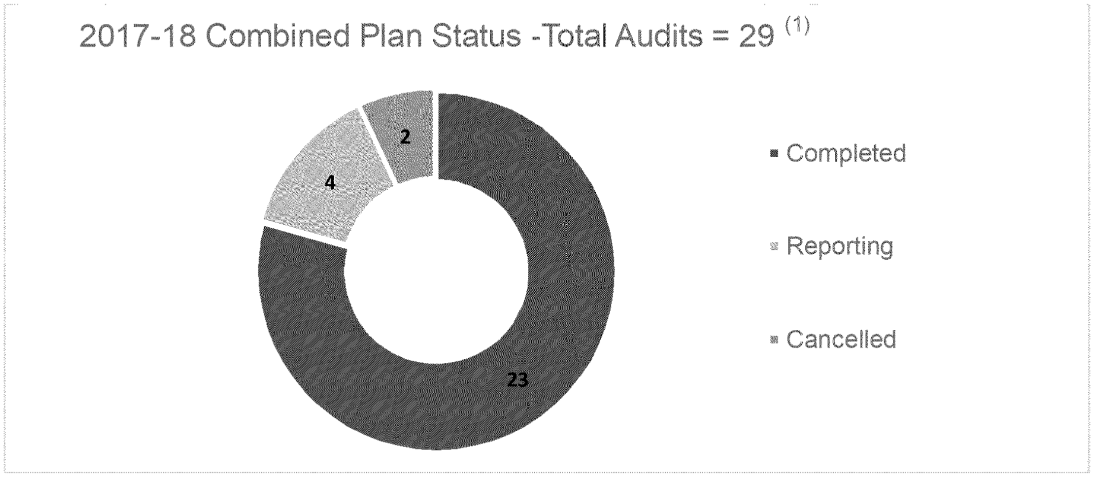
Questions this paper addresses

- Is the Internal Audit Plan on track? What progress has been made since the May RCC meeting?
- What progress is being made with completion of audit actions?
- Have any significant issues arisen that the committee should be aware of?

Conclusion

1. Progress against plan (2017-18):

Three reviews have been finalised since the May ARC meeting. The 2017-18 plan is now substantially complete with the last four reviews in the final stages of report clearance. Progress against plan is shown below:

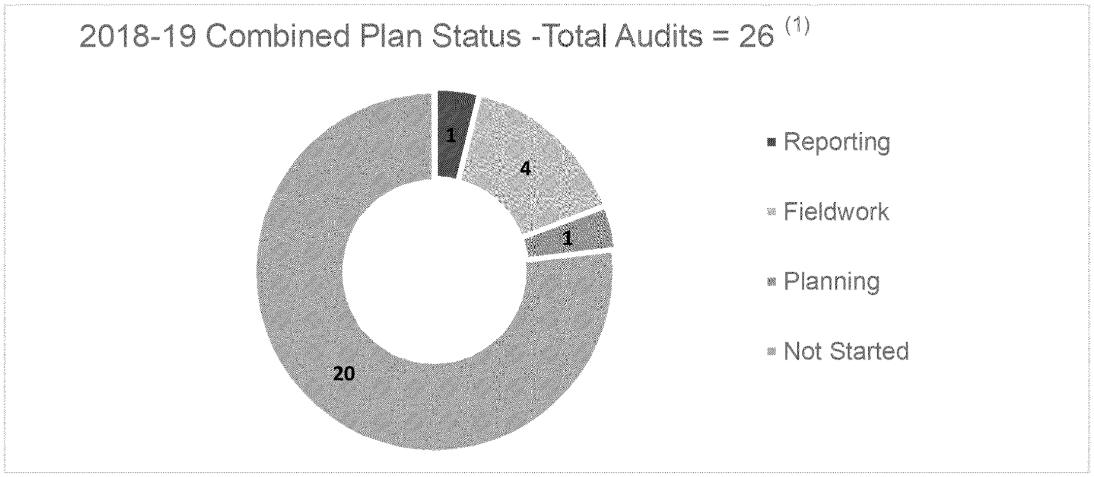


[1] ARC approved baseline plan for 2017-18 (16 internal control reviews & 13 change assurance reviews)

A full summary of the 2017-18 audit plan status is included in **Appendix 1**.

2. Progress against plan (2018-19):

Progress in Q1 has been slower than expected. This was due in part to two vacancies and the team finalising prior year audits, as well as resources being directed to the POMS audit plan and the team supporting other activities. Current delivery progress is as follows:



[1]ARC approved baseline plan for 2018-19 (16 internal control reviews & 10 change assurance reviews)

A full summary of the 2018-19 audit plan status is included in **Appendix 2**.

3. Open and Overdue Audit Actions (as at 29 June 2018):

Audit Action Status:	
Open (not yet due)	27
Overdue (<60 days)	12
Overdue (>60 days)	0
Total	39

More detailed information is provided in paragraphs 9 - 10 of the report.

4. Significant Issues:

There are no significant issues we believe the committee should be made aware of.

Input Sought

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

The Report

Changes to the Audit Plan since May RCC and ARC meetings

5. There was one addition to the audit plan:
    - Month-end Close Process – This is included in the core process rotation plan for 2019-20, but will be brought forward to the current year plan in light of the recent failure of month-end controls to identify errors in the accrued revenue for Telecoms.

Internal audit reviews completed

6. The following three reviews were finalised since the May ARC meeting:
    - EUM
    - Branch Technology
    - Business Continuity Management (BCM)

    Below are summaries of these reviews:

Audit	Key Messages
EUM In-flight review (Ref. 2017/18-05) Needs Improvement ***Sponsor:*** *Debbie Smith* Audit actions: P1 1 P2 3 P3 3 Total **7**	The objective of this review was to assess the level of confidence in delivery of the re-designed EUM solution that was approved by the Board in January 2018. We conclude that the EUM programme has made significant progress since the previous in-flight review. Project leadership has led the re-design of the solution and gained stakeholder support for the revised business case and solution. The composition of the Steering Committee has changed to include key stakeholders from affected programmes (e.g. HR Transformation), and effective governance is in place around delivery. However, there remain some key challenges that the programme will need to address and therefore this report has been rated 'Needs Improvement'. Specifically the audit found that: • The programme needs to focus on addressing the unwillingness of branches to adopt Smart IDs, and effectively manage its dependency on the Common Services Programme in relation to the data capture process, as the quality of the data provided by the latter is key to the rollout of Smart ID. • There is a requirement to have a high level of branch and business engagement to minimise intervention for data capture and support the migration to Smart ID and training compliance completion. The programme plan needs to be reviewed to ensure dates for design milestones are achievable, and underlying assumptions of the plan need to be validated once release dates from Fujitsu are received. • Formal go / no-go decision criteria needs to be defined which specifies the minimum thresholds for metrics for a positive go decision to be reached in respect of training controls.

Branch Technology
(Ref. 2017/18-26)

Needs Improvement

Sponsor:
Debbie Smith

Audit actions:

P1	0
P2	4
P3	3
Total	**7**

The Branch Technology project started in 2015 and was initially scheduled to deliver 22,500 counter terminals by June 2018 at a total cost of £49m. Costs have increased by 9% (circa £5m) as a result of an incorrect estimation of the number of terminals required (4,500 shortfall) and licensing costs. The objective of this review was to consider how the overall Branch Technology project is managed and whether it is on track to deliver successfully by September 2018.

Although the project has entered the latter stages of its lifecycle (now in the 26th month out of a proposed 30), there remains a significant volume of deployments outstanding, specifically 62% of counter terminals have not yet been deployed. The project team remains confident that deployments can be completed by September 2018, however, this audit has highlighted that the project is at risk of further cost and delays prior to deployment being completed, with insufficient governance and contingency in place to effectively mitigate these risks. Slippage past October 2018 would result in deployments being paused due to the 'change freeze' commencing in November 2018. If deployments are not completed by March 2019 then Fujitsu will have issues supporting the current application of HNGX beyond this date, resulting in additional costs ranging from circa £0.5m to £1.5m.

Key audit findings:

- There remain areas for improvement in the governance arrangements of the project, including ineffective risk and issue management and unclear roles and responsibilities.
- Delivery to the required timetable requires Computacenter to exceed contractual requirements of deployments per day - if contractual requirements were not exceeded, significant delays would occur.
- The required delivery rate of 80 branches per day at a 95% success rate has not been consistently achieved. Although ongoing monitoring is in place, deployment delivery timeline remains challenging with no contingency.

Business Continuity Management (BCM)
(Ref. 2017/18-17)

Needs Significant Improvement

Sponsor:
Jane MacLeod

Audit actions:

P1	0
P2	6
P3	1
Total	**7**

The objective of this review was to assess the adequacy of the BCM strategy, process and the BC plans as defined, including the design and operating effectiveness of controls in place.

There are areas of good practice in the BCM programme and some progress has been made in rolling out plans since the appointment of the current BC Manager. The BCM Policy is broadly aligned to the international standard (ISO 22301) and there is a high level of engagement from the Board Sponsor and Audit, Risk and Compliance Committee (ARC), who provide programme governance.

However, the review has identified areas where the BCM programme does not yet align to good practice or ISO 22301. Work is required to deliver alignment with the standard, and enable full management oversight of the BCM planning. The review identified a number of areas where work / effort is required. These include:

- There was a lack of visibility of where plans are held and their current status and it was difficult to obtain a clear understanding of the state of the BCM programme through

	documents and records; this may limit governance capability. • Key measures that support the robust and timely delivery of an adequate BCM programme and would enable the champions to deliver robust planning activity, has not yet been achieved. • Planning deliverables based on the current Business Impact Analysis (BIA) template may not provide management with the ability to confirm continuity and recovery prioritisations are correct, nor provide the planners with the focused information needed to deliver streamlined, joined-up BC plans. • PO is not yet exercising BCM plans effectively to assure itself that arrangements and plans that are in place will deliver the outcomes required, or identify areas of weakness. It is also falling short of current contractual exercising commitments expected by third parties. • There is no training material or approach in place to equip individuals across the business to deliver useful business continuity plans.

Reviews in Progress (2017-18 Audit Plan)

7. The following reviews from the 2017-18 audit plan are being finalised:

	Review	**Status / Remarks**
1	Telecoms Control Framework	Report being reviewed by management
2	Pension Schemes	Report being reviewed by management
3	IT Governance and Risk Management	Report being reviewed by management
4	Back Office Transformation (POLSAP Migration Re-plan)	Report being reviewed by management

Reviews in Progress / Planned (2018-19 Audit Plan)

8. The following reviews from the 2018-19 audit plan are in progress or being planned for delivery in Q2:

	Review	**Status**	**Timing[1]**
1	Procurement Fraud Investigation	Fieldwork nearing completion	30/04 - 15/07
2	Product Risk Review – Postal Orders	Draft report	30/04 – 25/06
3	Employee Expenses	Fieldwork	14/05 - 15/07
4	Change Governance Framework (Advisory)	Fieldwork nearing completion	02/05 – 15/07
5	DMB Strategy (Change Assurance)	Fieldwork	25/06 – 31/07
6	Payroll	Scheduled	August
7	Month-end Close Process	Planning	September
8	Cyber Security	Scheduled	September

[1] The timing of the reviews not yet in flight are currently being reviewed in light of the appointment of the new internal audit co-source provider.

Updates on Internal Audit Open and Overdue Actions

9. Following is the status of open and overdue actions:

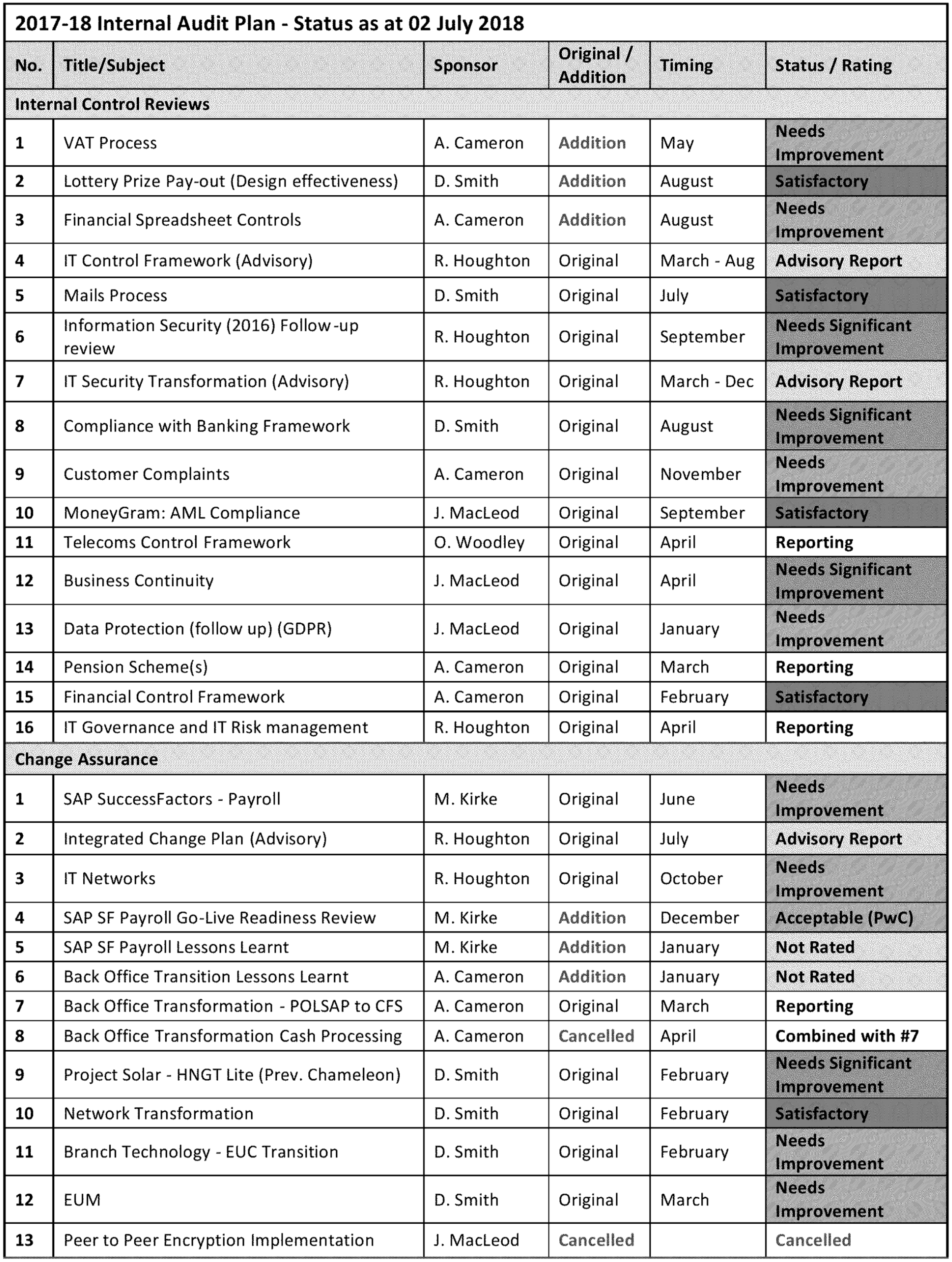
Audit Action Status at 29 June 2018:	BAU	Change	Total
Open (not yet due)	19	8	**27**
Overdue (<60 days)	0	12	**12**
Overdue (>60 days)	0	0	**0**
Total	19	20	**39**

10. Updates have only been received for two out of the 12 overdue actions and therefore we are unable to provide the reasons for actions being late or revised completion dates. These actions will now be escalated and verbal updates will be provided during the RCC meeting.

Description of action and Priority rating	GE Sponsor	Comments and Action Owners
EUM Programme		
7 actions overdue since 31 May 2108: 1 x P1 2 x P2	Debbie Smith	Updates requested on 1/06, 13/06 and 25/06. Update received from Claire Hurrell only. No updates from Julie Thomas, Esther Harvey and Chirag Kachalia.
Back Office Transition (Lessons to be Learned)		
1 P1 action overdue since 31 May 2018.	Rob Houghton	Updates requested on 1/06 and 13/06 from action owner, Tim White. No response received.
Project Mercury		
4 P1 actions overdue since 31 May 2018.	Debbie Smith	Updates requested on 1/06, 13/06. Update received from Jeff Lewis for his action. No updates received from Karl Oliver for his 3 actions.

END OF REPORT

Appendix 1



2017-18 Internal Audit Plan - Status as at 02 July 2018

No.	Title/Subject	Sponsor	Original / Addition	Timing	Status / Rating
Internal Control Reviews					
1	VAT Process	A. Cameron	Addition	May	**Needs Improvement**
2	Lottery Prize Pay-out (Design effectiveness)	D. Smith	Addition	August	**Satisfactory**
3	Financial Spreadsheet Controls	A. Cameron	Addition	August	**Needs Improvement**
4	IT Control Framework (Advisory)	R. Houghton	Original	March - Aug	**Advisory Report**
5	Mails Process	D. Smith	Original	July	**Satisfactory**
6	Information Security (2016) Follow-up review	R. Houghton	Original	September	**Needs Significant Improvement**
7	IT Security Transformation (Advisory)	R. Houghton	Original	March - Dec	**Advisory Report**
8	Compliance with Banking Framework	D. Smith	Original	August	**Needs Significant Improvement**
9	Customer Complaints	A. Cameron	Original	November	**Needs Improvement**
10	MoneyGram: AML Compliance	J. MacLeod	Original	September	**Satisfactory**
11	Telecoms Control Framework	O. Woodley	Original	April	**Reporting**
12	Business Continuity	J. MacLeod	Original	April	**Needs Significant Improvement**
13	Data Protection (follow up) (GDPR)	J. MacLeod	Original	January	**Needs Improvement**
14	Pension Scheme(s)	A. Cameron	Original	March	**Reporting**
15	Financial Control Framework	A. Cameron	Original	February	**Satisfactory**
16	IT Governance and IT Risk management	R. Houghton	Original	April	**Reporting**
Change Assurance					
1	SAP SuccessFactors - Payroll	M. Kirke	Original	June	**Needs Improvement**
2	Integrated Change Plan (Advisory)	R. Houghton	Original	July	**Advisory Report**
3	IT Networks	R. Houghton	Original	October	**Needs Improvement**
4	SAP SF Payroll Go-Live Readiness Review	M. Kirke	Addition	December	**Acceptable (PwC)**
5	SAP SF Payroll Lessons Learnt	M. Kirke	Addition	January	**Not Rated**
6	Back Office Transition Lessons Learnt	A. Cameron	Addition	January	**Not Rated**
7	Back Office Transformation - POLSAP to CFS	A. Cameron	Original	March	**Reporting**
8	Back Office Transformation Cash Processing	A. Cameron	Cancelled	April	**Combined with #7**
9	Project Solar - HNGT Lite (Prev. Chameleon)	D. Smith	Original	February	**Needs Significant Improvement**
10	Network Transformation	D. Smith	Original	February	**Satisfactory**
11	Branch Technology - EUC Transition	D. Smith	Original	February	**Needs Improvement**
12	EUM	D. Smith	Original	March	**Needs Improvement**
13	Peer to Peer Encryption Implementation	J. MacLeod	Cancelled		Cancelled

Note: Target audit delivery per original approved plan is for 29 audits (16 internal control reviews and 13 change assurance reviews).

POL00401627

Appendix 2

2018-19 Internal Audit Plan - Status as at 02 July 2018

No.	Title/Subject	Sponsor	Original / Addition	Timing	Status / Rating
Internal Control Reviews					
1	Product Risk Review (Postal Orders)	D. Smith	Original	April	**Reporting**
2	Employee Expenses	A. Cameron / J. Arakji	Original	April	**Fieldwork**
3	Procurement Fraud Investigation	A. Cameron	Addition	May	**Fieldwork**
4	Month-end Close Process	A. Cameron	Addition	Sept	**Planning**
5	Procure to Pay	A. Cameron	Original	Oct	Not Started
6	Payroll	A. Cameron / J. Arakji	Original	Aug	Not Started
7	Branch Cash Forecasting & Management	A. Cameron	Original	Q3	Not Started
8	Cyber Security	R. Houghton	Original	Sept	Not Started
9	Supply Chain Management (Logistics)	A. Cameron	Original	Nov	Not Started
10	Contract Management	A. Cameron	Original	Q3	Not Started
11	IT Control Framework	R. Houghton	Original	Oct	Not Started
12	Client Settlements Process	A. Cameron	Original	Oct	Not Started
13	Digital Strategy & Capability	O. Woodley	Original	Oct	Not Started
14	Whistle-blower Process (Grapevine)	J. MacLeod	Original	TBC	Not Started
15	Agents Remuneration	A. Cameron	Original	TBC	Not Started
16	Financial Control Framework	A. Cameron	Original	Q4	Not Started
Change Assurance[1]					
1	Change Programme Governance	R. Houghton	Original	May	**Fieldwork**
2	Payzone Business Integration	D. Smith / A. Cameron	Original	TBC	Not Started
3	DMB Strategy	D. Smith	Original	July	**Fieldwork**
4	Placeholder - Gold / Platinum Programme	TBC	Original	TBC	Not Started
5	Postmasters Portal	D. Smith	Original	TBC	Not Started
6	Identity Services	M. Edwards	Original	TBC	Not Started
7	Tracked Online/Disintermediation Risk	D. Smith	Original	TBC	Not Started
8	Customer Hub (Additional Verticals)	O. Woodley	Original	TBC	Not Started
9	Banking Framework - Cash Management	D. Smith	Original	TBC	Not Started
10	Project Everest	R. Houghton	Original	TBC	Not Started

[1] The list of Change Assurance reviews was approved by the ARC on the basis of being the highest risk programmes planned for 2018-19 at the time. The list will be reviewed and updated periodically to reflect the programmes most deserving of independent assurance.

Note: Target audit delivery per original approved plan is for 26 audits (16 internal control reviews and 10 change assurance reviews).

POST OFFICE

RISK AND COMPLIANCE COMMITTEE

Compliance Report

Author: Jonathan Hill Sponsor: Jane Macleod Meeting date: 10th July 2018

Executive Summary

Context

In April 2018, Post Office established a new combined compliance function within LRG, comprising Regulation and Compliance for our Financial Services and Telecoms businesses, Financial Crime compliance and Information Protection and Assurance.

It is anticipated that over the near future Compliance will encompass also regulation and compliance for the Banking, Payments, ATMs, Mails and Identity businesses and, working with IT Cyber Security, cyber-crime.

This papers sets out the first consolidated compliance report for Post Office Ltd.

Questions this paper addresses

- What are the regulatory/compliance regimes Post Office operates within?
- What are the key compliance issues and what is the business doing to address these?
- What is the forward-looking regulatory agenda?

Conclusion

The key compliance risk areas are;-

- Compliance with the Money Laundering Regulations and the remediation of Bureau de Change project requirements. We have already been fined by the HMRC for incorrect branch registrations and this area is being closely managed
- PCI DSS Compliance. Our mitigating actions are highlighted in the report. A key risk is compliance is required as part of our contractual commitment to the Banking Framework
- Meeting the future regulatory agenda. There are a large number of items featured in the regulatory appendix and the regulatory discussion continues to evolve. Of particular focus this year are the new General Condition requirements for Ofcom and the Insurance Distribution Directive which both come into effect in October and require substantial work together with other parties and Principals to ensure compliance
- The report below details how we are meeting these requirements

Input Sought

The Committee is requested to note this paper.

Confidential

Report

What are the principle regulatory/compliance regimes Post Office operates within?

1. Financial Services

    - Under the Financial Services and Markets Act (2000), Post Office is the Appointed Representative (AR) for Bank of Ireland UK plc (BoI) and from 1st October 2015, POMS; the latter for insurance. As the AR, Post Office is responsible for first line risk and compliance, working with BoI and POMS as the second line
    - This is overseen by the Financial Conduct Authority. Post Office Ltd has direct interaction with the FCA on an annual/twice yearly basis, as part of the FCA's supervision of BoI
    - Prudential Regulatory Authority. Post Office Ltd has direct interaction with the PRA on an annual/twice yearly basis, as part of the PRA's supervision of BoI
    - Payment Services Regulations (2017) – these regulate how payment services and electronic money are regulated in the UK. The PSRs are the UK's application of the EU's Payment Services Directive II ("PSD2"). They are overseen by the Payment Systems Regulator, which is part of the FCA. Under section 2.15 of the FCA's guidance on PSRs, along with a range of bodies such as banks and building societies, Post Office can provide payment services without the need for further authorisation or registration by the FCA

2. Telecoms

    - The telecoms regulatory regime is set out in the UK Communications Act (2003) and is overseen and enforced by Ofcom
    - Ofcom applies the standards for telecoms through its General Conditions, which are being revised. The updated conditions will apply from 1st October 2018
    - EU Telecommunications Single Market Regulation (2015) – net neutrality. This sets out guidance for providers about the use of their network and the data flowing through them. It also sets out the standards for information to be provided to customers (e.g., internet speeds). This is enforced through the UK's Advertising Standards Authority
    - Digital Economy Act (2017) – this gives Ofcom the authority to demand information to be produced by telecoms providers
    - Payment Services Regulations (2017) – Telecoms companies are also subject to the PSRs as a result of PSD2. Under PSD2, the purchase of physical goods and services (e.g., gambling sites) through a telecom operator now falls within the scope of the Directive. In order to avoid the risk of exposure to substantial financial risks to payers, only payments under a certain threshold are excluded (€50/£40 per transaction; €300/£250 per billing month). Telecom operators that engage in such an activity must notify PSR on an annual basis that they comply with these limits. The activity will also be listed in the public registers. We are investigating if Post Office's status as set out above applies also to our Telecoms business

3. Information Protection

- General Data Protection Regulations (2017) – This is the EU's update on EU Data Protection Directive (1996), harmonising and modernising data protection legislation across the EU
- UK Data Protection Act (2018) – embeds the GDPR into UK legislation
- In accordance with the DPA and GDPRs, Post Office has appointed a Data Protection Officer ("DPO"), Chris Russell. As part of the appointment, the DPO has a direct reporting line through to the Chair of the ARC in very serious cases
- Privacy & Electronic Communications Regulations ("PECR") (2003) – it regulates direct marketing the telecoms industry
- Articles 8 and 10 of the UK Human Rights Act (1998) – it sets guidance on how the State interacts with individual's privacy
- The above are all overseen and enforced by the Information Commissioner's Office ("ICO")
- ISO27001:2013 – this sets the standards for information security systems. This is three year certification and Post Office is assessed by an independent certification body (LRQ) on a six-monthly basis. Post Office's certification is due for renewal in 2019
- PCI-DSS – Payment card standards, set by Visa and MasterCard, enforced by the merchant acquirers. For Post Office this is Global Payments. This is an annual certification, with the security standards increasing year on year. We are independently assessed annually by a Qualified Security Assessor. For Post Office this is Nettitude

4. Financial Crime

- Proceeds of Crime Act (2002). It is the principal legislation for anti-money laundering in the UK. The Act has been amended since 2002, by the Serious Organised Crime and Police Act 2005, the Serious Crime Act 2007 and the Serious Crime Act 2015
- Money Laundering Regulations (2017) – these set the standards by which firms must seek to minimise the risk of money laundering and terrorism financing. Post Office is directly regulated by HMRC as a Money Services Business because of its travel money business

What are the key compliance issues and what is the business doing to address these?

Financial Services and Telecoms (including Banking Framework):

- The key compliance issues are reviewed by Post Office Compliance and its partners at the BoI Customer & Conduct Risk Committee, POMS Joint Compliance Committee, the Banking Framework Security, Compliance and Governance Committee Compliance and the Telecoms Compliance Committee. The key items for each are reported below:

5. BoI/Post Office Customer and Conduct Risk Committee (CCRC)

- The key customer and conduct risks were reviewed at the June CCRC. The Committee reviewed the conduct risk metrics contained in the Post Office Distribution Conduct Risk Dashboards and agreed they were within appetite. The CCRC meets every other month but with papers shared on a monthly basis
- One red metric for out of date literature (out of 12) was reported, which continues to be a challenge, although this has not resulted in material customer detriment. A range of mitigating actions have been implemented including producing a monthly Branch Focus communication, a Network-wide documented FS literature 'spot' check for Postmasters and Branch Managers to complete, which is then available for Network management to review upon visits. Also, the BoI Business Controls Team ("BCT"), together with the Post Office Conduct Compliance team is supporting the Network with literature compliance, as part of their agreed work plan
- However, we have also challenged the product teams to find more effective solutions for providing customers with product information
- Following the CCRC it was agreed that the BCT and Post Office Conduct Compliance teams would review MI in more detail (e.g., Quality of Sales Report and Work.com) to ensure that the BCT focuses its coaching work on the branches/areas of greatest risk
- Post Office Compliance has met with the BoI Vulnerable Customer Project Manager to discuss our respective work plans. We have initiated monthly meetings at a working level to communicate and where appropriate coordinate our efforts

6. POMS/Post Office Joint Customer and Conduct Risk Committee (JCC)

- The key customer and conduct risks were reviewed at the 2nd July JCC. The Committee reviewed the conduct risk metrics contained in the Post Office Distribution Conduct Risk Dashboards and agreed they were within appetite. The JCC meets monthly
- Two red metrics (out of 15) were reported and related to upheld complaints (related to customers not receiving their gift cards as part of the life promotion and is not branch behaviour related) and CRM Easy Life Insurance mystery shopping results, which continue to highlight a lack of conformance with the sales process. To address this VMS issue, additional training has been provided to the CRMs and their supervisors. The product team is looking at making simplification changes to the application process on the CRM tablets

Confidential

7. Additional Conduct Compliance activities

- The Conduct Compliance team's monitoring of the sale of FS&T products continues to develop ways of working to include the wider areas of compliance such as Information Security and Financial Crime
- Additional fact finding is being completed to understand how and what training is delivered/received in the non DMB branches in particular WHS branches. Initial feedback is that branches do not regularly go into Horizon to pick up the 'Branch Focus' communication which includes operations updates
- We are working the Network and L&D teams to build a robust training programme initially to be delivered in directly managed branches, but with the aim to use the content throughout the network

8. Banking Framework Security Compliance and Governance Committee (SCGC)

- Visa outages on 1st June and the importance of the Post Office network (which experienced an 8-10% uplift in cash demand) and access to cash as an alternative when other distribution fails
- Partner proposal for an external Audit on controls in framework following the Internal Audit that was recently undertaken was discussed
- Personal and Business Banking of branches within framework. It was agreed that Post Office should consider whether some form of best practice guidance needed to be considered for how Branches and their assistants could lodge money into their own accounts
- The SCGC meets on a quarterly basis and reports to the Banking Framework Steering Committee

9. Telecoms Compliance Committee (TCC)

- This is a new Committee which has been agreed with Fujitsu and will commence in July meeting every 2 months. The focus will be on current and future compliance with regulations. It will monitor progress and change to ensures risks are appropriately managed and there is transparency between us and our suppliers
- Removal of copper telephony product - Openreach has announced that they will remove WLR (our Homephone copper product) by 2025 and will replace this with alternative fibre products. Alongside these announcements Ofcom are consulting on new guidance for VoIP services which would be costly for Post Office and could result in forcing us to leave the Homephone market. We are lobbying both Ofcom and government accordingly
- Over the last two months there have been several data breach incidents in the telecoms business, principally as a result of the failure of our keys suppliers to effect proper controls and keep Post Office advised in a timely manner of such breaches. In all cases Post Office acted swiftly to limit the impact on our customers and minimise the business risk. The establishment of the Telecoms Compliance Committee will further strengthen our controls and oversight of the entire telecoms business chain
  - In one case, which Post Office reported to the ICO, we failed to meet the ICO's reporting timelines partly due to a reporting requirement interpretation difference and also due to the late advice from our suppliers. This will result in a fixed monetary penalty notice (£1,000) from the ICO,

which will be published on the ICO's website. In addition we have three similar cases pending, where the supplier failed to notify Post Office in time

10. Customer Hub

- The customer hub went fully live on 20th June with travel money and travel insurance. We have been working closely with the hub team to ensure a compliant delivery
- To this end we are establishing a monthly Enterprise Customer and Compliance Meeting. This Committee will seek to ensure that we obtain appropriate governance and control over tracking these issues whilst ensuring that we still remain part of an agile and digital working environment

Information Protection

11. General Data Protection Regulations ("GDPR")

- The GDPR came into force on 25th May 2018. Post Office delivered its 'effective compliance' programme before this deadline with the one significant exception of contract remediation that was reported to RCC previously
- The Programme has produced its strategy and plan for approval by the GDPR Steerco for 'substantive compliance' with a planned delivery date of the end of November 2018
- Since 25th May Post Office has received in excess of 300 Individual Rights requests, which is approximately 4 times the amount received in the previous year. All of these requests have either been dealt/on track to be dealt with in the statutory timescale of 30 days. The DPO and Head of Portfolio for LRG are monitoring this from a resourcing perspective
- In the first month of the new DP laws Post Office has seen a rise in the number of incidents that are being reported. As yet none of these, other than those within the Telecoms business that have different reporting requirements, have materialised into breaches that are notifiable to the ICO. The GE is kept up to date on all incidents through the weekly Incidents Report

12. PCI DSS

- There are daily progress meetings with Computacenter and twice a week with Fujitsu to ensure they remain on track with the BAU remediation actions
- To put the issues identified by the QSA into context, we believe that our environment has no Data or IT security exposures (as we have a locked down environment with no card data being forwarded from the device), but are issues related to compliance to PCI standards (matters related to monitoring and logging of device incidents). We remain in position to be able to take card payments from branches without our Attestation of Compliance (AoC)
- There are a number change requests that are being challenged by our supplier (Computacenter) and several legal letters have been exchanged on who is liable for costs
- Once our suppliers have implemented the necessary controls our QSA will be able to start its assessment and provide us our Report of Compliance (RoC) and AoC
- We have formalised all issues identified and are proceeding towards compliance with tight project governance. We are providing updates to our

acquiring bank of our progress and to date there have been no fines or additional charges applied and our relationship remains positive. We have been informed that there are a number of steps before fines are issued, with prolonged dialogue with our acquiring bank whereby they notify us of their intention

Financial Crime

13. Compliance with Money Laundering Regulations

- Annual AML/CTF training for Network and back office staff was delivered 4th – 30th May 2018. As at 27th June completion levels were 93.5% for Network and 95% for back office staff
- Non-conformance issues in the Network from 1st May to 22nd June 2018 included 52 incidents identified at 48 branches
  - 18 branches identified were Directly Managed Branches and/or WH Smith Multiples and these have been addressed by the Financial Crime Team and escalated to Network as appropriate
  - 13 branches remain on the non-conformance watch list following the new ID thresholds and will be manually monitored monthly until the new data environment is fully operational
- The volume of suspicious activity reports (SARs) May and June 2018, was stable (c. 258 in May and c. 150 to 22nd June), and reports relating to bureau de change are increasing overall – most of these from internal monitoring rather than branch reports

14. Travel Money & HMRC

- We have written to HMRC to set out our legal interpretation of and approach to Customer Due Diligence and Fit & Proper requirements under the 2017 MLRs and await their written response, however at a meeting on 21st June the Director General advised us that HRMC agreed with our interpretation of the regulations for Customer Due Diligence, removing the need for us to capture copies of customers' ID. However, the DG also advised that HMRC is holding to its reporting requirements for vetting and Fit & Proper, although she agreed that HMRC would be as practical as possible
- The HR Fit & Proper project team is continuing to progress actions as previously agreed with our HMRC supervisor. Significant work is now required to write to all agents to obtain missing information and their self-certification
- During work on the Fit and Proper data, it was identified that a number of branch premises had been registered incorrectly (41 branches with an 'out of scope' branch type) or not de-registered as required (19 branches). These branches will be notified to HMRC as de-registrations, but it was too late to prevent the annual registration fee for these being processed in June
- The Credence universe data environment for bureau de change was transferred to live on 15th June with c52K records which had not been identified during the extended testing phase. These have subsequently been resolved. Transaction monitoring reports are being finalised and will be phased in over the next six months

Confidential

- eKYC, PEPs and Sanctions capability went live on 22nd June for all transactions over £2k, with results appended to the transaction data in the Credence universe to enable monitoring and investigation as required

15. Financial Crime Risk Assessment current status

- 19 Product Information Packs received in May and June (Mobile Phone Top Ups, Postal Orders, Travel Money Hub, (9)Partner Banking Framework, Bill Payment Pre Paid Cards, Drop and Go, gift Cards, MoneyGram, Bill Payments, Multi-Currency Card and International Payments)
- 14 Financial Crime Assessments completed in May and June (4 initial risk assessments via the assessment tool – Business Cash Encashment, POCA, Amazon Top-Up, Travel Money Hub. 10 full Financial Crime Assessments – Partner Banking Framework, Bill Payment Pre Paid Cards)
- 9 draft Financial Crime Assessments issued to product managers for review and sign-off in May and June (Partner Banking Framework)
- No Product Information packs overdue/7 due in July and August (PaySafe Cash, Amazon Top-ups, POCA, Business Cheque Encashment, Current Accounts, Savings, Bureau de Change)
- No risk assessments overdue/3 due in July and August (Current Accounts, Savings, Bureau de Change)
- PO Insurance products were due for reassessment in May. Thistle Initiatives assessed these last year, however there were no PIPs completed at that time. A workshop was help in May with PO Insurance to assist with PIP completion and we are awaiting receipt

16. Anti-Bribery and Corruption (ABC) update

- No material non-conformance issues to report. Please refer to separate annual Gifts & Hospitality report and annual policy review and assurance paper
- Annual ABC training is due to be rolled out from 27th July 2018

17. Whistleblowing update

- No material non-conformance issues to report. Please refer to separate annual Whistleblowing report and annual policy review and assurance paper

18. Regulatory updates

- The update relating to the Fifth Money Laundering Directive in the January report remains current
- The impact of and response to the recent US withdrawal from the Joint Comprehensive Plan of Action (JCPOA) with Iran is being assessed via UK Finance, UK and EU regulators and governments. There may be consequences in relation to transactions with individuals travelling in Iran. Post Office continues to engage via UK Finance to determine impacts

19. External threats

- The Travel Money Card was subjected to a sustained BIN card number generation attack in May that impacted c. 5,340 cards/customers (c. 97k card authorisations were attempted online). Cards have been blocked and re-issued. FRES is working with the outsource card processing platform provider

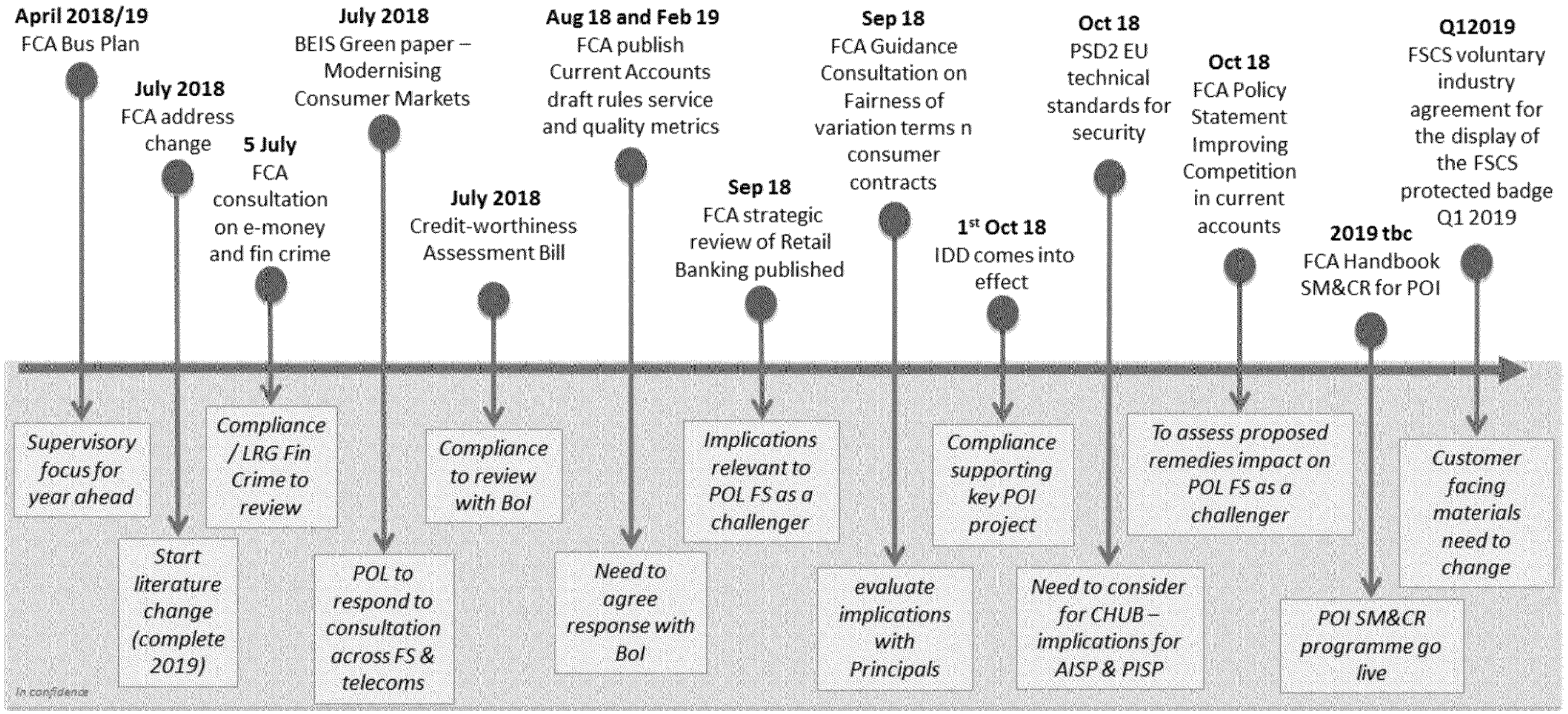
FIS to ensure its authorisation and detection system rules are able to block these type of attacks

- This is not a new style of attack, but illustrates that criminals will exploit known modus operandi and system weaknesses

What is the forward-looking regulatory agenda?

20. The tables below set out the key activities of the Financial Services and Telecoms regulators. As we develop this we will look to include calendars for Financial Crime and Information Security regulation.

Post Office Financial Services Regulatory Calendar



April 2018/19
FCA Bus Plan

Supervisory focus for year ahead

July 2018
FCA address change

Start literature change (complete 2019)

5 July
FCA consultation on e-money and fin crime

Compliance / LRG Fin Crime to review

July 2018
BEIS Green paper – Modernising Consumer Markets

POL to respond to consultation across FS & telecoms

July 2018
Credit-worthiness Assessment Bill

Compliance to review with BoI

Aug 18 and Feb 19
FCA publish Current Accounts draft rules service and quality metrics

Need to agree response with BoI

Sep 18
FCA strategic review of Retail Banking published

Implications relevant to POL FS as a challenger

Sep 18
FCA Guidance Consultation on Fairness of variation terms n consumer contracts

evaluate implications with Principals

1st Oct 18
IDD comes into effect

Compliance supporting key POI project

Oct 18
PSD2 EU technical standards for security

Need to consider for CHUB – implications for AISP & PISP

Oct 18
FCA Policy Statement Improving Competition in current accounts

To assess proposed remedies impact on POL FS as a challenger

2019 tbc
FCA Handbook SM&CR for POI

POI SM&CR programme go live

Q12019
FSCS voluntary industry agreement for the display of the FSCS protected badge Q1 2019

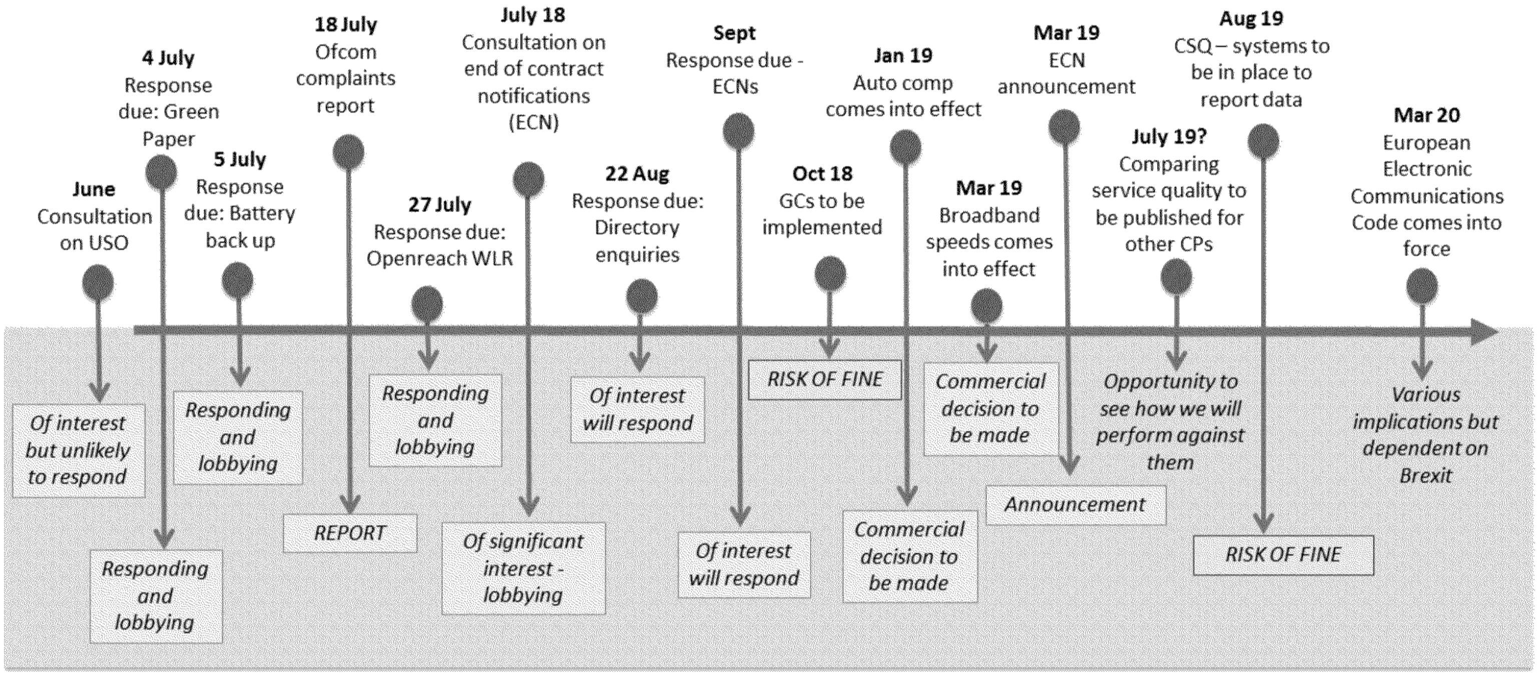
Customer facing materials need to change

In confidence

Supplementary Documents

POST OFFICE LIMITED RISK AND COMPLIANCE COMMITTEE-10/07/18

Post Office Telecoms Regulatory Calendar



June Consultation on USO – *Of interest but unlikely to respond*

4 July Response due: Green Paper – *Responding and lobbying*

5 July Response due: Battery back up – *Responding and lobbying*

18 July Ofcom complaints report – *REPORT*

27 July Response due: Openreach WLR – *Responding and lobbying*

July 18 Consultation on end of contract notifications (ECN) – *Of significant interest - lobbying*

22 Aug Response due: Directory enquiries – *Of interest will respond*

Sept Response due - ECNs – *Of interest will respond*

Oct 18 GCs to be implemented – *RISK OF FINE*

Jan 19 Auto comp comes into effect – *Commercial decision to be made*

Mar 19 Broadband speeds comes into effect – *Commercial decision to be made*

Mar 19 ECN announcement – *Announcement*

July 19? Comparing service quality to be published for other CPs – *Opportunity to see how we will perform against them*

Aug 19 CSQ – systems to be in place to report data – *RISK OF FINE*

Mar 20 European Electronic Communications Code comes into force – *Various implications but dependent on Brexit*

Confidential

Next Steps

21. We will look to develop a single Compliance dashboard as we develop greater MI capabilities in the business

22. As set out in the introduction, we anticipate that Compliance will encompass also regulation and compliance for the Banking, Payments, ATMs, Mails and Identity businesses and, working with IT Cyber Security, cyber-crime

Jonathan Hill

Compliance Director

July 2018

POST OFFICE
RISK AND COMPLIANCE COMMITTEE

Vulnerable Customers Risk Assessment and Gap Analysis

Author: Jonathan Hill Meeting date: July 2018

Executive Summary

Context

1. The Post Office agreed its Vulnerable Customer Policy in September 2017. This recognised that Post Office is already assisting vulnerable customers in a wide variety of ways reflecting our social mandate.

2. As part of this policy it was agreed that Post Office would undertake a risk assessment during 2017/18. This work was to enable Post Office to identify any gaps in how it supports vulnerable customers and identify good practice.

3. The assessment would also highlight potential solutions in areas where there are gaps identified.

4. We also provided an update and response to the FCA's Ageing Population paper to the Committee in January 2017.

Questions this paper addresses

5. This paper updates the Committee on the assessment. Attached are

- Appendix 1, the assessment,
- Appendix 2 the proposed work plan,
- Appendix 3 the vulnerable customer policy.

Conclusions

6. The overall picture from the review is that Post Office does a huge amount to support customers in a wide variety of vulnerable situations. However, to date Post Office has not been able to present these as a coordinated approach/position.

7. The risk assessment has identified some key required improvements as well as some other items that we could take forward.

8. Key items we are actioning include.

- Required re-organisation and improvement in providing branch literature in an alternative format to vulnerable customers

Strictly Confidential

- Provision of discounted text relay services for Telecoms customers (an Ofcom requirement).
- Compliance with wider Ofcom 'General Condition' rule requirements for vulnerable customers
- Improving our training and awareness of vulnerability across the business
- Reorganisation of vulnerable customer and social responsibility pages on the Post Office website

Input Sought

The Committee is asked for feedback generally and to support the proposed actions in the work plan.

The Report

The Scope of Vulnerability in the UK

9. Significant groups in our communities are impacted either temporarily or permanently by vulnerability. For example;
   - There are 850 thousand people in the UK with dementia and this is expected to rise to a million over the next three years (Alzheimer's Society 2018)
   - In any given year one in four of the adult population suffers a mental illness (NHS 2017)
   - Over 2 million people in the UK are coping with sight loss (RNIB 2015)
   - 6.5 million People in the UK have caring responsibilities. Carers UK predict this will rise to 9m by 2037 (Carers UK 2014)
   - Every 2 minutes someone in the UK is diagnosed with cancer (Cancer Research UK 2014)
   - By 2020 half of the UK can be expected to be diagnosed with cancer at some time in their lives (Macmillan 2014)
   - One in 7 adults has literacy skills of a child aged 11 or below:
   - Just under a half of the population has numeracy attainment skills of a child aged 11 or below (Department of Innovation Business and Skills 2012)

   What is important is that as well as the impact vulnerability has on the individual, the impact spreads widely across family and friends and the wider community who provide care and support to that person.

The Government and Regulatory Context

10. The Government and regulators have put increasing emphasis on ensuring that society does more to ensure that vulnerable customers are protected.

    April 2018 Green Paper issued by the Department for Business, Energy and Industrial Strategy' 'Modernising Consumer Markets'.

    Vulnerability is a key theme in the paper. The Green paper states that '*regulators should act robustly to prevent harm to vulnerable customers and design systems* *that work for vulnerable customers. Companies must understand their customers including those who are vulnerable, and how they can reasonably support their needs'*

One specific area where government wants to see action is in helping consumers with mental ill health, cognitive impairments and dementia including conditions like Alzheimer's'.

11. <u>Ofcom</u>

12. Ofcom has had for some time a number of requirements in relation to vulnerability for example, fault repairs have to give priority to the needs of those with disabilities. These vulnerability requirements have increased following the issuing of the latest regulations (General Conditions) that apply from October 2018.

13. <u>FCA</u>

14. Consumer vulnerability is a key priority for the FCA. As well as the Occasional Paper on Vulnerability that was published in 2015. The FCA's 2018/19 Business Plan states that vulnerability and exclusion will form a key part of their future approach to consumer regulation.

15. <u>The challenges for the vulnerable, the business opportunity and the market response</u>

16. The various regulatory and charity research papers have highlighted the challenges the vulnerable face in accessing goods and services. As well as the obvious physical dexterity and mental challenges; these hurdles can be attitudinal. With the increased number of older and vulnerable members in society together with the support network, getting this right is also an important business opportunity. The vulnerable and the supportive community are customers and potential customers (see below)

17. '*You feel invisible. At the perfume counter the staff ignore me because I am an older woman with a stick. But if I'm with my daughter they are there in a flash. I have the money, I want to buy mascara and make-up but the staff ignore me. They don't think someone like me wants to wear mascara.*' (Female, Newcastle Age UK)

18. The Business Disability Forum 'Walkaway Pound Report' 2015 asked people whether they had left a shop or business because of poor disability awareness or understanding: three quarters (75%) of people with a disability and their families said that they had done this. The forum calculated the headline figure of £1.8 billion per month being lost to businesses that were not disability smart.

19. Vulnerability is an issue our competitors are taking seriously:

- Barclays Bank has focussed on improving the experience for the vulnerable. This includes 'B pay', wearable technology (wristbands, jewellery) to facilitate payments for those that struggle with dexterity, sight problems or dyslexia. As well as clearly signposted support for those with sight, hearing or dexterity problems across the consumer facing business areas. This includes branches giving demonstrations on how to use products and the digital eagles' service to help people get more from the internet.

- BT has a dedicated vulnerability team and a dedicated website ('including you') they undertake roadshows and undertake a regular Consumer Group Forum with vulnerable charities to get feedback on how their services can be improved.

Listening and working with our stakeholders

20. We have engaged with a number of stakeholders to understand the challenges raised by their members and what improvements they would like to see:

- We have engaged with key stakeholders including, Sense, Mind, Alzheimer's Society, Age UK and UK Finance the industry trade association.
- The Alzheimer's Society has reviewed some of our training and we have been in dialogue with the needs of their members. This has included information on the 'Dementia Friends' programme and how Post Office could take part.
- Discussed with the CEO of the NFSP his commitment to vulnerable customers and his support for initiatives such as 'Dementia Friends' and ' Just a Minute (JAM)' cards to enable those who may struggle to communicate to let people know discretely and easily that they just need a little more time.
- We have opened up on an opportunity to work with Sense, together with their accessibility champions to user test the Post Office Customer Hub
- We have joined two relevant industry groups in relation to Financial Services Provision, the Personal Banking Product and Services Board Vulnerability Sub Group and the Financial Inclusion and Capability Working Group to ensure we learn from best practice

How are we meeting the challenge in key areas?

21. Overall the work has shown that we can demonstrate that Post Office takes its responsibilities to vulnerable customers seriously.
22. For example;-

- Numerous examples of community outreach and partnerships with local charities/vulnerable customers made through Agency branches. For example the case featured in the 'Post Office One' with Pontrillas branch that set up a group to combat loneliness and to visit elderly people at home.
- The Banking Framework is a key demonstration of how Post Office is supporting elderly and vulnerable customers. We are increasingly the last 'bank' in town as bank branches close supporting those who prefer to do their banking in branch with the additional support that Post Offices can offer at the counter.
- A Banking process currently exists for DDA/vulnerable customers when they are unable to use the chip & Pin functionality.
- POca serves to meet the needs of the most vulnerable in society including the 'unbanked' and 'financially excluded' through facilitating government payments into a cash account with proprietary card access
- Bill payments operates as a key service for vulnerable customers. In particular the unbanked and those financially excluded. Ability to pay bills via the SSK gives vulnerable customers additional support through trained staff on hand.

23. There are some areas that require immediate action to meet our obligations to the vulnerable which are set out within the next section. We will look to do this within existing budgets where possible.

Key areas-what more we need to do

24. Alternative format literature

25. The provision of alternative format branch literature (e.g., large print, braille, audio) appears to be non-functional in some areas. This has been tested for Credit Cards, Mortgages, Travel Insurance, Home Insurance, Pre Paid Funeral and Telco (Retail is undertaking testing of its products).

26. The test identified that the helpline operators are unaware of the process for supporting these customer needs. This leads to a poor experience for our vulnerable customers and would be looked at critically by our regulators.

27. It is proposed FS&T Compliance will drive a project, working with product managers, and marketing that will;-

- Define what we should offer vulnerable customers in alternative format
- Ensure that we deliver consistent solutions to this, working with third party suppliers as required.

28. Telecoms Text Relay service

A text relay service is used by customers on landlines with communication difficulties. Although we have a text relay service, we are non-compliant as we do not offer discounted rates for this service, which is required by Ofcom. A plan is in place to make these changes working with our supplier, Fujitsu.

29. New Ofcom General Condition Requirements

Ofcom has introduced new requirements for the treatment of vulnerable customers as part of its General Conditions refresh. These regulations come into force in October 2018. We are required to publish a Telecoms Vulnerability Policy on our website.

The new regulations also mean that we have to take into account more transient types of vulnerability e.g. bereavement and divorce. Previously, the regulations were focused on the treatment of customers with disabilities (the provision of discounted text relay and the supply of large print/braille bills).

A work plan is in place to meet the all new General Condition requirements related to vulnerability by the required date of October 2018.

30. Training our staff and the Network (including Dementia Friends)

31. There is some existing guidance in place across the Network as part of the Accessibility Guide 2014 (this has recently been re-reviewed by accessibility consultants see Appendix). The annual compulsory FS workbook and test, also includes a limited learning section/question on vulnerability as well as the Telco training materials.

32. We intend to build on this with a specific module on 'vulnerable customers' on Success Factors that will be available for all our employees.

33. We are also working together with the NFSP on communications and initiatives for our Agents with the Alzheimer's Society-and the 'Dementia Friends' initiative. The Alzheimer's Society materials and the 'Dementia Friends' initiative is something we are considering taking forward as the training messages given (about taking more time, listening etc.) are generic to most vulnerable groups.

34. The Alzheimer's Society will be able to recognise our training as creating Dementia Friends if it meets their criteria and we report back numbers who complete the training regularly.

35. Communication on the Post Office Website

The current vulnerability information is difficult to find on the Post Office website. The existing information needs to be updated as there are some out of date references. One of our priorities is giving better direction and support for the bereavement/Power of Attorney Process. We also need to improve our information on avoiding scams, working together with the BoI.

It is proposed that together with the Marketing and Digital teams, we incorporate the Post office's approach to supporting vulnerable customers in a new social responsibility and community pages, looking to go live August 2018.

Proposed Next Steps and the way forward

Following re-organisation changes, the new co-sponsors of this work are the Network and Sales Director Roger Gale and the Compliance Director Jonathan Hill.

The next steps are to take forward the action plan across the Post Office and continue our work on vulnerability working with our stakeholders where required and continuing to learn about best practice.

Jonathan Hill
Director of Compliance

Strictly Confidential

Vulnerable Customers

Assessment of approach towards 'Vulnerable Customers'

24/06/18

Extract from Post Office Vulnerable Customer Policy September 2017

'By not addressing the needs of vulnerable customers, the impact could be significant for those customers that depend on us to deliver our products and services….It could also cause reputational damage undermining Post Office's achievement of its social purpose. Under both Ofcom and FCA rules there could be regulatory interventions for not treating vulnerable customers fairly.'

Red	Key area that needs resolving and work plan unclear. Prompt resolution required to meet our requirements for customers, non-compliance could have regulatory or reputational impact
Amber	Issues identified and work plan in place, no breach provided actions delivered as planned
Green	No current customer or compliance issues identified but there may be work plans (some significant) to improve our offering/proposition

Vulnerable Customers

Which areas	What we know (how we support customers)	Reg/Legal Regt	Suggested actions	RAG Status	By Who (Owner)
Branch Accessibility	• Branch Accessibility Guidelines. There is a good Network management understanding of the accessibility requirements branches need to adhere to particularly through NT. • There is comprehensive guidance on this provided in a document dated March 2014 covering ;- • Disability and the Equality Act • Post Office's Accessibility Standards and Guidance • Further Sources of Help and Advice • An Accessibility Assessment Form • The assessment of Retail is that this guidance is well understood by the Network Lead Team.	Yes-DDA reqts	We have recently asked our external Accessibility Adviser and our legal team to help us update the guidelines. Once available we need to work with the Communications Team and Network to work through how this should be re-communicated particularly the messages about how to identify and assist vulnerable customers. We are aware the Direct Enquires site (The Nationwide Accessibility Site) does not have up to date information on Post Offices. We are working to update this with our suppliers. Once updated we should link this to Post Office Corporate site.	**Green**	**Martin HopCroft Date Sep 2018** **Network (TBA)** **Network**
Network	Numerous examples of community outreach and partnerships with local charities/vulnerable customers made through Agency branches. For example the case featured in the 'One' with Pontrillas branch that set up a group to combat loneliness and to visit elderly people at home.	No	Work with marketing to see how these good news stories could feature on our website.	**Green**	**FS&T Risk and Marketing (June2018)**

Vulnerable Customers

Which areas	What we know (how we support customers)	Reg/Legal Regt	Suggested actions	RAG Status	By Who (Owner)
Propositions General. Consideration of Vulnerability for new Projects	For some FS products we undertake a Consumer Detriment Risk Assessment (CDRA) to review whether a new or changed proposition or distribution method could have a potential detrimental effect on customers. But it is unclear how this is undertaken for other propositions.	Yes (FCA/Ofcom)	We ensure that as part of our Gating Process there is a step to challenge on whether vulnerable customer requirements are relevant and if so whether they have been considered	**TBC**	**TBC**
Propositions **Mails**	• Although we do not own or control the specifications of our mails products, our supplier, Royal Mail (RM) has a good track record in this area. RM provide: • Literature in braille • Welsh language options • Hard of hearing helpline support • POL acts to signpost these RM services to customers who need them. • RM also has an 'articles for the blind' service. If the recipient of the mail is blind then the sender can post free of charge. This service must be offered as part of the Universal Service Obligation • As part of our contract with RM we must have a least one host to 4	No	From a product perspective there is very little we can change as they belong to RM. Citizens Advice has recently submitted a report for review related to Postal Services. PO to review and consider if there are any lessons learned as a result of this,	**Green**	**James Scutt to review and follow up with mails team**

Vulnerable Customers

Which areas	What we know (how we support customers)	Reg/Legal Regt	Suggested actions	RAG Status	By Who (Owner)
	SSKs. Hosts are not there to specifically help vulnerable customers but are able to offer support if required. Likewise mails transactions are all available over the counter which is an assisted sale. RM also offer a Special Circumstances mails redirection service for those with power of attorney seeking to redirect mail on someone elses behalf. This service is not free.				
Government Services	**POca:** POca serves to meet the needs of the most vulnerable in society including the 'unbanked' and 'financially excluded' through facilitating government payments into a cash account with proprietary card access. The customer base split between 'working age' claimants and 65+ pensioners. The service distributes large volumes of cash through our branch network and serves as a significant part of our social purpose by providing a critical service to the financially excluded. Monthly statements are available in the following formats: • Braille	No	The rollout of Universal Credit (UC) and a changing competitive landscape are the key drivers of change. POca becomes an unsuitable product for customers under UC due to the limited functionality and increased claimant financial responsibility to manage funds, which cannot be supported on the existing product. There has been a shift in the financial services industry targeting the 'unbanked' and 'financially excluded', fuelled by regulation and government policy on Financial Inclusion. The market is evolving with the rise of challenger banks, increased pressure on traditional high	**Amber**	**Ross Borkett** **Pilot Q4** **Launch Q1 2019/20**

Vulnerable Customers

Which areas	What we know (how we support customers)	Reg/Legal Regt	Suggested actions	RAG Status	By Who (Owner)
	• Large print • Audio CD		street banks to provide basic bank accounts and the continued presence of Credit Unions. The Future of POca programme seeks to address the current challenges through the development and delivery of new solutions that will replace the current POca service, better serve our customers and meet the requirements of DWP. The Future of POca programme seeks to achieve the following outcomes: • Maintain and grow the number of financially excluded customers we serve (either directly or through our banking framework). • Continue to drive footfall into our branch network and support the retailer proposition. • Support our wider cash and ATM strategies. • Deliver a sustainable profit.		

POL00401627

Vulnerable Customers

Which areas	What we know (how we support customers)	Reg/Legal Regt	Suggested actions	RAG Status	By Who (Owner)
			• Continue to be one of the main providers of services to the financially excluded while also helping customers avoid the poverty premium.		
Payment Services	**Bill Payments:** Bill payments operates as a key service for vulnerable customers. In particular the unbanked and those financially excluded. Ability to pay bills via the SSK gives vulnerable customers additional support through trained staff on hand. **ATMs:** • Fundamental POca access route to cash outside of POL branch opening times • Mobile phone top ups for PAYG customers • Talking functionality • DDA compliant • Upgraded machines now dispense £10 polymer notes which have braille on them • Mixture of Internal ATMs as well as External machines to help provide additional	**Yes DDA**	**None identified**-Paul Wordsworth and Public Affairs have responded (June 2018) to the Energy UK Commission for Customers in Vulnerable Circumstances. The Commission will be independently chaired, by Lord Whitty and will explore how standards of care and support for vulnerable customers can be improved. The Commission will report by the end of 2018, and make recommendations for industry, Government and other stakeholders. In addition to the work of the Commission, Energy UK will be separately developing a new 'Vulnerability Charter' to build on existing commitments	**Green**	

Vulnerable Customers

Which areas	What we know (how we support customers)	Reg/Legal Regt	Suggested actions	RAG Status	By Who (Owner)
	security/privacy to those who require it - Free to use balance inquiry/mini statement **Non-Cash Payments:** - PACE system in place (the authorisation of transactions via a signature rather than pin pad from other banks. Eg: Lloyds counter cash withdrawal made via card and signature - Full ergonomic assessment of pin pads has been undertaken in relation to supporting people with disabilities: conclusion is that the pin pad is reasonably accessible and usable, although there are issues that have been identified for those with a serious sight issue - Braille on pin pad		and go further to support customers most in need. Our intention through this engagement is to position the Post Office as being a key cornerstone in how the UK Energy Industry supports Vulnerable Energy Customers in paying their bills.		
Identity	**Verify:** Product needs to be improved to provide specific support to aid those customers that are excluded from financial and other services because of the difficulties in passing ID checks.eg the usual passport plus utility bills etc.	No	This is a significant challenge and business opportunity. Delivery road map in place, working with UK Finance and regulators to ensure approach is aligned to industry requirements and there is scope for sharing a central ID standard.	**Green**	**Bryn Robertson Morgan** **Ongoing Programme through to 2019**

Vulnerable Customers

Which areas	What we know (how we support customers)	Reg/Legal Regt	Suggested actions	RAG Status	By Who (Owner)
	Digital Check and Send: No need to write/take photo/sign etc. Transaction handled by the agent. Photo booths are set up to cater for people with disabilities.				
Banking Framework	The Banking Framework is a key demonstration of how Post Office is supporting elderly and vulnerable customers. We are increasingly the last 'bank' in town as bank branches close supporting those who prefer to do their banking in branch with the additional support that Post Offices can offer at the counter. Banking team are proactively looking to work with Credit Unions, Homeless charities for vulnerable people, where they have no relationship with the mainstream banks. A Banking process currently exists for DDA/vulnerable customers where they are unable to use the chip & Pin functionality. Bank approaches team in Bristol to agree a mandate with the PO branch to make cheque encashment e.g. 3 times a week for £100.	No	Five point plan to promote Banking Framework including enhanced support for vulnerable customers following Citizen's Advice Guidance. FS&T Compliance are working with UK finance on the vulnerability principles to follow working together with CAB	**Green**	**Martin Kearsley- and FS&T Compliance Sep 2018**

Vulnerable Customers

Which areas	What we know (how we support customers)	Reg/Legal Regt	Suggested actions	RAG Status	By Who (Owner)
PO Money products	Post Office Money target customer segments are not age-based but are attitude based and include older customers' needs, particularly in the first two categories of our three target segments (Prosperous and Discerning, Socially Responsible) We have product propositions aimed at older customers, including products for end of life planning (savings, pre-paid funeral, over 50s life, life assurance and home insurance). Our latest product propositions are specifically considering the needs of older customers, including an intergenerational mortgage Post Office Family Link and a freedom mortgage Post Office Retirement Link. The Retirement Link product is specifically designed for those that need to access capital from their home (for example, for later life planning or care costs) without having to sell up or downsize. We are also evaluating savings and lending propositions for those that have cash flow needs including those that may be caring for generations above and below them; or for those that need funds to cover care costs. The regulator has also tacitly acknowledged that its application of	Yes (FCA guidance)	FS&T Risk have recently joined two working groups as part of our membership of UK Finance a Vulnerability Sub Group and the Financial Inclusion and Capability Working Group. We will assess what best practice is in the industry and feed back to FS&T and Post Office as required.	**Green**	**Jonathan Hill ongoing**

Vulnerable Customers

Which areas	What we know (how we support customers)	Reg/Legal Regt	Suggested actions	RAG Status	By Who (Owner)
	regulations (particularly for mortgages) has led to product providers excluding access to older customers for regulatory reasons. In this new climate we are working with BoI on re-evaluating the upper age limit for lending products. Power of attorney process was reviewed and updated in Dec 2016 with support pages on Horizon help (but see below actions)				
BOI supplier of Post Office Money products	BoI has a specific team and programme assigned to vulnerable customers and they are plugged in to industry initiatives. Mandatory training for all BoI staff and additional training for customer facing areas eg call centres. Notifications of bereavements and POA requests are processed by a specialised team. Vulnerability consideration taken into account for premature PO Money bond closure eg divorce, redundancy Unusual levels of withdrawals are monitored and blocked. PO Money Mortgages – specialist team to support customers when faced with	Yes (FCA guidance)	The UK's biggest high street banks and building societies agreed to implement a new set of Principles in line with **'*Easy for friends and family to support'* –** designed to improve processes around the registration and use of legal instruments that can be used to enable third party access to financial affairs such as Power of Attorney, Court of Protection Orders to Appointees and Guardianship Orders. Firms including BoI are targeting March 2019 for implementing changes to their current propositions, where these might not presently meet the minimum standard. The mandate can also be adjusted	**Green**	**PO Money and BoI (March 2019 for third party access initiative)**

Vulnerable Customers

Which areas	What we know (how we support customers)	Reg/Legal Regt	Suggested actions	RAG Status	By Who (Owner)
	~~A~~ arrears, missed payments and a change of circumstances that could impact on the keeping up with the Mortgage payments. Customers are encouraged to act first before going into arrears to prevent impacting on their credit history. PO Money – Credit Cards – letters are sent to customers when the minimum payment is only paid for 6/12 months only explaining the risks.		to describe the minimum proposition for single product providers. This could support friends and family when there is a need to assist or reach out to the bank for help during emergencies such as hospitalisation or other short-term situations of need – all those unplanned circumstances, which might require the assistance of a trusted party to help in paying the bills.		
Post Office Insurance (POMS)	Post Office Insurance has recently put together a high level paper on its approach to vulnerability in an ARC paper. As part of the response it is enhancing call centre training using material from the Alzheimer's Society.	Yes (FCA guidance)	Review FCA feedback statement in Summer 2018 relating to challenges for Firms and consumers in providing and accessing fairly priced cover for people with pre-existing medical conditions for any actions.	**Green**	**Ian Holloway POMS (Sep 2018)**
Travel Money and MoneyGram	Training is given to branch colleagues to help with the identification of 'Scams' for our vulnerable customers for MoneyGram transactions. A number of transfer requests are identified and stopped by branch colleagues, eg September 58 frauds 41% customers were considered vulnerable re Romance scams, a Medical emergency or utility refund.	Yes (HMRC)	Continue to raise awareness of scams on vulnerable customers and good news stories where postmasters have protected them from crime.	**Green**	**Comms team ongoing**

Vulnerable Customers

Which areas	What we know (how we support customers)	Reg/Legal Regt	Suggested actions	RAG Status	By Who (Owner)
Telecoms	Ofcom have introduced new requirements for the treatment of vulnerable customers as part of their General Conditions refresh. These regulations come into force in October 2018 and require us to publish a Vulnerability Policy on our website. The new regulations also mean that we have to take into account more transient types of vulnerability e.g. bereavement, divorce. Previously the regulations were focused on the treatment of customers with disabilities (the provision of discounted text relay and the supply of large print/braille bills). Currently, we identify Elderly and Vulnerable customers ("EVPs") and offer priority fault repair. This process is not comprehensive enough and requires an element of self-identification. We would not categorise someone as vulnerable just because of their age. Telco have undertaken pro-active measures to identify vulnerable customers but further work still needs to be done. For example an initiative to get Care line numbers matched up with Local Authorities help, as a result	Yes (Ofcom)	The Post Office currently only has one category on the system, EVP. New regulations mean that we have to take into account more transient types of vulnerability e.g. bereavement, divorce. We need to be able to tailor our treatment of vulnerable customers according to their needs i.e. not everyone should qualify for free priority fault repair. We also need to ensure that call centre staff have sufficient training to deal with the different categories identified. We need to consider how we should split out customers into different categories so that it's clear if they are "vulnerable" customers and what specific treatment they should receive to meet their needs.	**Amber**	**Meredith Sharples Oct 2018**

Vulnerable Customers

Which areas	What we know (how we support customers)	Reg/Legal Regt	Suggested actions	RAG Status	By Who (Owner)
	of this work an additional 4000 cases were identified. Where someone has currently been recorded as "EVP" they receive: • be-spoke approach to collection cycle for bad debts (exclusion from Dunning process). • Delegated authority process (to help if customer can't respond) • prioritisation for fixes and faults • special treatment for pricing changes (Project Galaxy)		As part of this, we plan to review the training and handling of our vulnerable customers. Following this we need to ensure we have a detailed internal procedural document and a public policy that outlines what we do at a higher level. This will be Teleco specific but should be tied into the wider PO policy. Branch staff should also receive vulnerability training across the network and not just training specific to Telco.		
Telecoms	Although we have a Text Relay service, we are non-compliant as we do not offer discounted rates, and this requires a system change. A CR has been raised and this is being progressed by Fujitsu.	Yes (Ofcom)	Fujitsu are implementing a fix to address the current issue.	**Red**	**Meredith Sharples Need to agree timescales with Fujitsu**
Customer Hub	This important innovation needs to take into account the needs of vulnerable customers. Whilst many	Yes (FCA) WCAG	New customer hub. User testing will includes all kinds of user testing including those	**Green**	**Henk Van Hulle. Sep 2018**

Vulnerable Customers

Which areas	What we know (how we support customers)	Reg/Legal Regt	Suggested actions	RAG Status	By Who (Owner)
	vulnerable groups may be tech savvy, many are not. As at June launch MVP01 is not meeting accessibility standards, however Hub does have a plan in place to address this issue.		that are not tech savvy and testing will seek to get a wide range of ages for testing. Charity 'SENSE' have offered testing resource for the Customer HUB 1. To confirm the accessibility standards we are required to meet for an APP. June 2018 2. To agree timetable to meet these. July 2018 3. To engage Sense in user testing after this. Sep 2018		
Communication	**PO Website** **Web Accessibility:** The Accessibility Consultant for Post Office has confirmed that the general digital accessibility standards are adhered to within PO and with our partners (BOI, FRES, Royal London, Aviva etc.-) The Post Office accessibility standards were written 2008 but they are based on WCAG 2.0 (Web Content Accessibility Guidelines) which are an international standard	Yes WCAG	These standards are being revised this year. We have a consultant working with the committee who are developing the revised guidelines (WCAG 2.1) and as result will feed in any key changes to coincide with them being released which means we should be completely up to date with.	**Green**	**Rob Wemys July 2018**

Vulnerable Customers

Which areas	What we know (how we support customers)	Reg/Legal Regt	Suggested actions	RAG Status	By Who (Owner)
Communication	PO Money has on the website some useful information such as Help with Bereavement page which contains the following contacts; • General Register Office for England and Wales opens in new window • Probate & Matrimonial Office opens in new window • National Association of Funeral Directors opens in new window • Citizens Advice Bureau opens in new window • Money Advice Service opens in new window • StepChange Debt Charity opens in new window • National Debt line opens in new window • Debt Advice Foundation opens in new window • Department Of Work and Pensions opens in new window • HM Revenue & Customs Linked to this page are other areas of support; Redundancy, Divorce & Separation, Caring for others finances.	Yes FCA	• PO Money VC pages hard to find. Liaise with Marketing to align and make visible our VC messages. • Some corrections to bereavement pages required. One of our priorities is giving better direction and support for the bereavement/Power of Attorney Process. We also need to improve our information on avoiding scams, working together with the BoI. • New content pages on avoiding scams to be inserted. • Work with Communications team to assess whether a more fundamental re-organisation of the vulnerability information is required alongside our existing information about community etc	**Amber**	**Andrew Ellis PO Money August 2018** **FS&T Risk to raise with Comms team June 2018.**

Vulnerable Customers

Which areas	What we know (how we support customers)	Reg/Legal Regt	Suggested actions	RAG Status	By Who (Owner)
	Post Office has also • Screen reader on One website • Communication on mental health, wellbeing shared online.				
Communication Network	• One off Network communications have been issued on various issues such as dementia awareness in Branch Focus/Team Talks etc • Scam prevention initiatives working together with Age UK and local Police Forces to prevent vulnerable and elderly customers succumbing to frauds • NFSP have communicated to its network details about vulnerable communities and the work postmasters undertake	No		**Green**	
	Written Materials The communications we make to customers are generally as clear and easy to understand as possible. Working with outside agencies as required.		We are noted by 'Crystal Mark' as being members of the Clear English Scheme. We have not established whether we continue to meet these standards or whether we should display this mark on our communications in different media.	**Amber**	**FS&T Risk to take forward with marketing** **July 2018**
	Written Materials/brochures **Communication Materials**	Yes (FCA)(Ofcom)	FS&T risk will drive a project plan working with product managers, owners.	**Red**	**Product Owners in FS&T and Marketing**

Vulnerable Customers

Which areas	What we know (how we support customers)	Reg/Legal Regt	Suggested actions	RAG Status	By Who (Owner)
	The provision of alternative format (eg large print, braille) appear to be broken for FS&T products. This has been tested for Credit Cards, Mortgages, Travel Insurance, Pre Paid Funeral, Home Insurance and Telco. The helpline numbers are not functional and the process appears broken. Generic Here to Help Leaflet doesn't mention availability of any alternative formats		1. Complete testing on other products to see extent of impact on areas outside of FS&T 2. Define what we are going to offer vulnerable customers in alternative format 3. Ensue that we deliver the consistent solution to this working with third party suppliers as required.	▨	**1. James Scutt July 2018** **2. FS&T Compliance working with Retail/FS&T** **3. TBC**
Training and Awareness	There is existing guidance in place across the Network as part of the Accessibility Guide 2014 The annual compulsory FS workbook and test also includes a learning section/question on vulnerability as well as the Telco training materials. The SF 'Delivering a Great Customer Experience' Module has significant training on Vulnerable Customers. Customer Relationship Managers CRMs are trained on vulnerable customers and provided with back up material in paper format for customers	Yes (FCA) (Telco)	We have asked Alzheimer's Society for feedback on our existing training We are considering further training options both through Success Factors for our employees and through alternative methods to our Agents. The Alzheimer's Society materials and the 'Dementia Friends' initiative is something we are considering taking forward as the training given is generic to most vulnerable groups. Design , build and roll out a bespoke VC training module, L & T team have been engaged	**Green**	**FS&T Risk to take forward with Training** **July 2018**

Vulnerable Customers

Which areas	What we know (how we support customers)	Reg/Legal Regt	Suggested actions	RAG Status	By Who (Owner)
	that can't relate to tablet technology. CRM training covers VCs.		and are carrying out this work stream to be delivered into the business in parallel to the new web architecture launch. (key sections will be POA, Probate & Bereavement) **Suite of Videos –** 5 Available, the 'reading and writing' module was filmed within a Post Office. Branch can register on website, receive a unique code which can be watched either individually or as a team. Information can be provided via post codes of where they are being used and who has taken the training. We are also working together with NFSP on communications and initiatives for our Agents with the Alzheimer's Society- and 'Dementia Friends' this initiative is something Royal Mail currently participates in. Any new module in Success Factors to be made available to CRMs as part of Compliance training.		

Vulnerable Customers

Which areas	What we know (how we support customers)	Reg/Legal Regt	Suggested actions	RAG Status	By Who (Owner)
Customer Insight and Experience	Insight team receive feedback from around 1300 customer survey responses per month, within the advocacy programme. Identification of any customer vulnerabilities would be acted upon but none known as time of review.	**No**	**None identified**	**Green**	
NBSC	Jane Smith and Lisa Cawthorne who look after calls from the branch network (NBSC). Product specific issues are directed to the 'Here to Help' leaflet Where customers have access issues reported e.g. wheelchairs, they make local arrangements with the Branches, and by using the branch doorbell to make the branch aware they require assistance. Branches do refer/report any physical branch changes requirements, through the management line.	**No**	To make additional VC training available to NBSC through Success Factors. We will do this by sharing our new VC bespoke training module.	**Green**	**FS&T Risk to take forward with marketing** **July 2018**
Social Media	Our Social Media team has confirmed from a monitoring tool perspective that our system picks up vulnerability buzzwords, and prioritises those posts (aka shows them higher up the queue so they get a faster response time). The Lithium will pick up things that were directly posted onto Facebook,	**No**	**None identified**	**Green**	

Vulnerable Customers

Which areas	What we know (how we support customers)	Reg/Legal Regt	Suggested actions	RAG Status	By Who (Owner)
	twitter, LinkedIn etc. However, if these posts have been made in internet forums, we don't get sight of them. Lisa Cawthorne and Jane Smith have confirmed, once escalated, the Social team respond to the tweets and posts. They will request information to be sent them via email to ensure a full resolution of the issues. They will refer to proposition manager within PO/BOI/POMS, where applicable.				
Complaints	Whilst individual complaints/feedback relating to vulnerability are taken forward it is unclear whether we undertake any trend analysis and learn from them, this is also the case from complaints dealt with by Post Office, BoI. POMS or elsewhere.	Yes-FCA (DISP) Ofcom	Undertake complaints assessment to review whether any more work can be undertaken both through Post Office and third parties to review trends we can learn from.	**TBC**	FS&T Compliance to drive some further exploratory work to assess whether we can do more to learn from our complaints **TBC 2018**
Branch and Staff guidance on how (or whether) to approach the authorities where we are concerned for customers in different circumstances	There have been some occasions when it has been unclear what the protocol should be(if any) for alerting the authorities to protect a vulnerable customer (for example an individual that continually tried to deposit and withdrew tiny amounts of cash from a non-serviced account and was acting confused when help was being offered).	No	Work further with Charity sector to understand practicalities of this. If guidance can be provided we will work this Comms team.	**TBC**	FS&T and Public Affairs to drive some exploratory work on this with our Charity contacts **TBC 2018**

Vulnerable Customers

Which areas	What we know (how we support customers)	Reg/Legal Regt	Suggested actions	RAG Status	By Who (Owner)
e.g. customers with mental illness, or those that are subject to protection orders etc					

Vulnerable Customers work plan

Summary Vulnerable Customer work plan.

This does not cover items already planned to take place as part of our strategy or business planning (eg such as the Identity Programme or the future of POCa work).

This is divided into

1. Work we have to do for regulatory or key stakeholder management.

2 Optional work-nice to haves

3. Challenging things

Vulnerable Customers work plan

1.What we have to do (for regulatory or key stakeholder management).

Which areas	Summary Detail	Reg/Legal Regt	Work plan	Is there a budget consideration?	By Who (Owner)
Branch Accessibility	- Branch Accessibility Guidelines. In place but need updating (2014)	Disability and the Equality Act	Accessibility Adviser has given us feedback on the guidelines. Once available we need to work with the Communications Team and Network to work through how this should be re-communicated particularly the messages about how to identify and assist vulnerable customers. We are aware the Direct Enquires site (The Nationwide Accessibility Site) does not have up to date information on Post Offices. We are working to update this with our suppliers. Once updated we should link this to Post Office Corporate site.	**None expected for the assessment work, TBC for any required changes.**	**Martin HopCroft Date July 2018**
Banking Framework	A key part of the Five point plan to promote Banking Framework includes enhanced support for	Yes-FCA (PSRs)	Post Office is working with UK Finance to agree general	**No budget issues**	**Martin Kersley-Paul Beaumont Sep 2018**

Vulnerable Customers work plan

Which areas	Summary Detail	Reg/Legal Regt	Work plan	Is there a budget consideration?	By Who (Owner)
	vulnerable customers following Citizen's Advice Guidance.		vulnerability principals to be followed.		
Telecoms	Ofcom _new vulnerable customer requirements October 2018	Yes (Ofcom)	The Post Office currently only has one category on the system, EVP. New regulations mean that we have to take into account more transient types of vulnerability e.g. bereavement, divorce. We need to be able to tailor our treatment of vulnerable customers according to their needs i.e. not everyone should qualify for free priority fault repair. We also need to ensure that call centre staff have sufficient training to deal with the different categories identified. We need to consider how we should split out customers into different categories so that it's clear if they are "vulnerable" customers and what specific treatment they		**Meredith Sharples Oct 2018**

Vulnerable Customers work plan

Which areas	Summary Detail	Reg/Legal Regt	Work plan	Is there a budget consideration?	By Who (Owner)
			should receive to meet their needs. As part of this, we plan to review the training and handling of our vulnerable customers. Following this we need to ensure we have a detailed internal procedural document and a public policy that outlines what we do at a higher level. This will be Telco specific but should be tied into the wider PO policy. Branch staff should also receive vulnerability training across the network and not just training specific to Telco.		
Telecoms	Although we have a Text Relay service, we are non-compliant as we do not offer discounted rates, and this requires a system change. A CR has been raised and this is being progressed by Fujitsu.	Yes (Ofcom)	Plan in place to address the current issue.	**None expected**	**Meredith Sharples** **Need to agree timescales with Fujitsu**
Communication	**PO Website**	Yes WCAG	These standards are being revised this year. We have a	**Not known**	**Rob Wemys** **July 2018**

Vulnerable Customers work plan

Which areas	Summary Detail	Reg/Legal Regt	Work plan	Is there a budget consideration?	By Who (Owner)
	Web Accessibility: The Accessibility Consultant for Post Office has confirmed that the digital accessibility standards are adhered to within PO and with our partners (BOI, FRES, Royal London, Aviva etc.-) The Post Office accessibility standards were written 2008 but they are based on WCAG 2.0 (Web Content Accessibility Guidelines) which are an international standard.		consultant working with the committee who are developing the revised guidelines (WCAG 2.1) and as result will feed in any key changes to coincide with them being released.		
Communication	PO Money website requires significant updating on social responsibility and vulnerability	Yes FCA	• PO Money VC pages hard to find. Liaise with Marketing to align and make visible our VC messages. • Some corrections to bereavement pages required. One of our priorities is giving better direction and support for the bereavement/Power of Attorney Process. • We also need to improve our information on avoiding scams,	**Within existing budgets**	**Andrew Ellis PO Money Sep 2018**

Vulnerable Customers work plan

Which areas	Summary Detail	Reg/Legal Regt	Work plan	Is there a budget consideration?	By Who (Owner)
			working together with the BoI. • New pages on avoiding scams to be inserted. • Work with Communications team to assess whether a more fundamental re-organisation of the vulnerability information is required alongside our existing information about community etc. • Work with Comms to see how all these good news stories from the Network could feature on our website.		
	Written Materials/brochures **Communication Materials** The provision of alternative format (eg large print, braille) appear to be broken for FS&T products. This has been tested for Credit Cards, Mortgages, Travel Insurance, Pre Paid Funeral,Home Insurance and Telco. The helpline numbers are not	Yes (FCA)(Ofcom)	FS&T Compliance will drive a project plan working with product managers, owners. 1. Close testing on other products to see if these impact on other areas outside of FS&T 2. Define what we are going to offer vulnerable customers in alternative format	**Yes, to be determined by solution that needs to be put in place.**	**Product Owners in FS&T and Marketing** **July 2018**

Vulnerable Customers work plan

Which areas	Summary Detail	Reg/Legal Regt	Work plan	Is there a budget consideration?	By Who (Owner)
	functional and the process appears broken. Generic Here to Help Leaflet doesn't mention availability of any alternative formats		3. Ensue that we deliver the consistent solution to this working with third party suppliers as required.		
Training and Awareness	To improve our vulnerable customer training across the network. 1. For our employees via a new SF module 2. For the wider Network through initiatives with the NFSP	Yes (FCA) (Telco)	1. Plan in place for FS module 2. We are also working together with NFSP on communications and initiatives for our Agents with the Alzheimer's Society- and 'Dementia Friends' this initiative is something Royal Mail currently participates in.	**Within existing budget**	**L&D Sep 2018**

2. Optional work-nice to haves

Which areas	Summary Detail	Reg/Legal Regt	Work plan	Is there a budget consideration	By Who (Owner)
Proposition (Gating)	To consider vulnerability in all our customer facing propositions	Various eg DDA, FCA, Ofcom etc	Review whether the gating process should include as part of the 'gate' customer vulnerability considerations before new projects go live	**Yes- Potentially depending on any proposition changes to accommodate**	**Paul Beaumont FS&T Compliance Sep 2018**

Vulnerable Customers work plan

Which areas	Summary Detail	Reg/Legal Regt	Work plan	Is there a budget consideration	By Who (Owner)
				vulnerable customers	
Customer Hub	To meet industry best practice for accessibility. Then for this to be tested by the charity Sense.	Yes (FCA) WCAG	This has been factored into MVPO1 post launch	**Within CHUB budget**	**Henk Van Hulle** **July 2018**
Communication material	We are noted by 'Crystal Mark' as being members of the Clear English Scheme.	No	We have not established whether we continue to meet these standards or whether we should display this mark on our communications in different media.	**Not known**	**FS&T Compliance to take forward with marketing** **July 2018**

3. Challenging things

Branch and Staff guidance on how (or whether) to approach the authorities where we are concerned for customers in different circumstances e.g. customers with mental illness, or	Social responsibility. There have been some occasions when it has been unclear what the protocol should be (if any) for alerting the authorities to protect a vulnerable customer if we are concerned about their welfare. (Whilst if someone exhibits threatening behaviour or is threatening their own life there are obvious actions to take relating to contacting the police)	No	Work further with Charity sector to understand practicalities of this. If guidance can be provided we will work this Comms team.	No expected budget implications	LRG Compliance and Public Affairs to drive some exploratory work on this with our Charity contacts **Sep 2018**

Vulnerable Customers work plan

those that are subject to protection orders etc					
Complaints	Whilst individual complaints/feedback relating to vulnerability are taken forward it is unclear whether we undertake any trend analysis and learn from them, this is also the case from complaints dealt with by Post Office, BoI. POMS or elsewhere.	Yes-FCA (DISP) Ofcom	Undertake complaints assessment to review whether any more work can be undertaken both through Post Office and third parties to review trends we can learn from.	No budget currently for this activity	A start would be for LRG Compliance to drive some further exploratory work to assess whether we can do more to learn from our complaints **Aug 2018**

Vulnerable Customer Policy

Version – Final 1.0

Group Oversight Committee:	Audit and Risk Committee
Sign-off Authority:	Risk and Compliance Committee
Policy Sponsor:	Kevin Gilliland and Nick Kennett
Policy Owner:	Tom Weschler and Jonathan HIll
Policy Author:	Paul Beaumont and Jonathan Hill
Approved by:	
Approved:	25.09.2017
Next review:	25.09.2018

1. Overview

1.1. Introduction by the Policy Owner

At the Post Office we are committed to providing quality products and services for all our customers. We work in an open and responsible way that builds the trust and respect of all our customers. Post Office seeks to ensure that all customers are provided with good product and service choices, so that they can make good buying decisions and have a positive experience when dealing with us.

Addressing the needs of vulnerable customers is core to Post Office's social purpose and is aligned to our objectives to be 'Better for Customers' and a 'Great Place to Work'. There are countless examples of how we assist customers when they need us most. This policy outlines the policy approach so that we continue to ensure that we are able to look after the needs of vulnerable customers.

1.2. Purpose

To articulate Post Office's expectations as to how employees and agents identify and help vulnerable customers during their interaction with the Post Office its products and services. This will also be an important document and source of information on Post Office's policy approach for many of our stakeholders.

1.3. Core Principles

Much of consumer protection legislation is underpinned by the notion of the average or typical consumer, and what they might expect, understand or how they might behave. Some consumers may be significantly less able to represent their own interests, and more likely to suffer a greater risk of customer detriment than the average consumer, with regard to achieving the most appropriate price, service, product or quality available to them. This may be for a variety of reasons, as outlined below (this list is not exhaustive).

Vulnerability can impact in many ways and these categories are examples. The Post Office recognises that these customers may have additional needs and may be described as 'vulnerable' although it is important to note that these customers may not regard themselves as such. It is core to Post Office's rationale and purpose to ensure that appropriate respect and care is taken of all types of customer, including vulnerable customers.

Categories include:

A. Restricted Mobility
B. Communications Needs
C. Low Basic Skills
D. Low Financial Capability
E. Mental Capacity
F. Age Related Vulnerability
G. Life Event Vulnerability
e.g., bereavement, critical illness, redundancy
H. Financial Difficulties

1.4. Application

There are already many examples of how Post Office assists vulnerable customers these include:

- Improving disabled access and fitting hearing loops
- Team talks on vulnerability
- Financial Services and Telecoms training on vulnerability e.g., "Delivering a Great Customer Experience", "General Compliance" training modules and the "Compliance Training Manual for Broadband and Phone"
- Training on mental health awareness risk
- Participation in National Police initiatives to mitigate frauds on vulnerable customers
- Rolling out the Banking framework to ensure financial access to communities including the vulnerable when bank branches are closing
- Our response to the Grenfell Tower fire and ensuring we could support customers in time of emergency
- Working with partners such as BoI who give case by case exceptions to the 'terms of conditions' for customers, for example customers in hospital unable to read banking correspondence and statements, or those that have suffered a bout of mental illness.

Post Office provides advice and guidance to customer-facing staff and those involved in the design of products and services and the processes that support their distribution and sale, regarding the legal requirements, regulatory guidance and relevant industry body recommendations, as well as Post Office recommended best practice.

It is the responsibility of those staff to ensure that they comply with and observe those requirements or guidance, and where there is any uncertainty, to seek clarification from relevant Post Office subject matter experts.

1.5. Risk

By not addressing the needs of vulnerable customers, the impact could be significant for those customers that depend on us to deliver our products and services. These risks are included in the minumum control standards section below but could include customers not being able to access our products or services, inappropriate purchases and not being able to understand the features or terms and conditions of a product or service.

It could also cause reputational damage undermining Post Office's achievement of its social purpose. Under both Ofcom and FCA rules there could be regulatory interventions for not treating vulnerable customers fairly.

1.6. Legislation

- Ofcom duties under the Communications Act

- Disability Discrimination Act 1995
- Equality Act 2010
- Mental Capacity Act 2005 and guidance
- Power of Attorney Act 1971
- Disability Discrimination Act (Northern Ireland) 2005.
- Adults with Incapacity (Scotland) Act 2000.
- Consumer vulnerability regulation detailed within the FCA Handbook for CONC and Mortgage Conduct of Business (MCOB).

1.7. Industry Guidance

- FCA website including 2016 Thematic Review on vulnerable customers
- ABI/BBA Codes of Practice
- Age UK advice line
- Money Advice Service
- Pensions Advisory Service

2. Risk Appetite and Minimum Control Standards

2.1. Risk Appetite

A Risk Appetite is the extent to which the Group will accept that a risk might happen in pursuit of day to day businesses transactions. It therefore defines the boundaries of activity and levels of exposure that the Group are willing and able to tolerate.

Post Office's risk appetite is **averse** for:

- non-compliance with law and regulations or deviation from its business conduct standards, and
- for taking risks which might result in failure to maintain the service commitment in respect of customers in line with our social purpose and Government's policy on subsidy.

The Group acknowledges however that in certain scenarios even after extensive controls have been implemented a product or transaction may still sits outside the agreed Risk Appetite. In exceptional circumstances a Risk Exemption waiver may be granted.

2.2. Policy Framework

Post Office's Board has overall responsibility for ensuring that Post Office has a framework to ensure compliance with legal, regulatory and contractual requirements. The Board is kept abreast of relevant matters relating to the management of vulnerable customer matters by reports from its committees including its Audit and Risk Committee.

It is the responsibility of the policy owners to review this policy at least once a year and on an ad hoc basis as necessary to ensure the policy remains effective and up to date.

This policy will be reviewed by The Post Office Risk and Compliance Committee at least once each year from the last date this policy was determined effective.

2.3. Who must comply?

Compliance with this policy is mandatory for all Post Office employees. We will work with our Agency network, Principals and key commercial partners to ensure that where we can the spirit of our approach to vulnerable customers is applied.

2.4. Minimum Control Standards

A minimum control standard is an activity which must be in place in order to manage the risks within the defined Risk Appetite statements contained within the table below. To comply with this, mechanisms must be in place within each business unit or product to demonstrate compliance. The minimum control standards can cover a range of control types, i.e. directive, detective, corrective and preventive which are required to ensure risks are managed to an acceptable level and within the defined Risk Appetite.

The minimum control standard for the vulnerable customer policy is 'directive' and will be communicated to staff through staff communications and intranet.

We should maintain the existing training requirements that we have in place (for example this is covered in the annual Horizon FS handbook training, Team Talks and the 'Delivering a Great Customer Experience module' on Success Factors) and aim to build on this where we can to ensure that our approach is regularly communicated.

The table below sets out some of the key relationships between identified risk, the considered Risk Appetite, and the required minimum control standards:

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible
Physical access to the branch network is difficult	**A) Restricted Mobility** A customer may be particularly vulnerable because they have mobility restrictions; this means that it might be difficult for them to gain physical access to our premises.	• We will seek to, where it is possible to do so, make 'reasonable adjustments' to our business premises to allow customers with mobility restrictions to access our business premises. • Where we are not able to make such adjustments we will seek, where it is reasonable to do so, to provide the customer with an equivalent service through other means.	Kevin Gilliland / Al Cameron
Customer engagement with products and services is not possible or limited because of a vulnerability	**B) Communications Needs** A customer may be particularly vulnerable because they have a hearing or sight impairment, which means they require specially adapted methods of communication.	• We will look to make 'reasonable adjustments' to the way in which we are able to communicate with our customers. For instance for sight impairment, we will seek to ensure that our customer documentation is available in a range of formats to help them understand our product material and product-life cycle communications • For hearing impairment, we will seek to provide hearing loops, and for our telephony staff, training in use of telephone relay technology.	Kevin Gilliland / Nick Kennett Al Cameron / Kevin Gilliland
	C) Low Basic Skills A customer may be particularly vulnerable because they have a low level of basic skills (including not having English as a first language) and therefore require additional or specialised assistance to effectively make use of our products and	• We will seek to work positively and constructively with customers that have, or appear to have, a low level of basic skills. • We will seek to ensure that the use of jargon is minimised within our documentation. Where it is used we aim	Kevin Gilliland / Nick Kennett

POST OFFICE LIMITED RISK AND COMPLIANCE COMMITTEE-10/07/18

Supplementary Documents

	services or, during the course of the product life-cycle, interact with us and manage their financial position effectively.	to ensure that there is an easy to understand explanation of the term. • We will look to provide sign-posting to free independent sources of information and support that the customer can access in relevant documentation and sections of our websites. • We will seek to explore how to simplify the information that we provide to customers, for example, through the standardised terms and conditions to highlight parts that matter. If appropriate we will engage with government and industry initiatives	
	D) Low Financial Capability A customer may be particularly vulnerable because they have a low level of financial capability (e.g. a specific lack of the maths skills and knowledge of financial products or matters) and therefore may require more straight-forward explanations.	• We aim to be clear and fair and not misleading in communications with customers, and wherever possible we will seek to avoid 'jargon'. We will strive to explain our products and services, including associated risks to customers, in a manner which is easily understandable. • We will seek to take reasonable steps to ensure there is sufficient 'sign-posting' across our product and service proposition to charities and other not-for-profit organisations that provide independent advice and guidance on financial issues	Kevin Gilliland / Nick Kennett
	E) Mental Capacity A customer may be particularly vulnerable because they have a mental capacity limitation (for instanced dementia, a learning disability, a development disorder,	• Be aware of the Power of Attorney requirements where applicable (refer to Horizon Help) • We aim in our dealings with a customer who we know, or reasonably suspect has	Kevin Gilliland/ Nick Kennett

	a neurological disability) that may restrict their ability to appropriately engage with us or make an informed and responsible borrowing decision.	a mental capacity limitation, to act sympathetically and positively. • We seek to allow a customer sufficient time to weigh-up the information and explanations we have provided and defer a decision to a later date. We will seek to provide all the information required to enable a customer to do this. Where possible we should ask if the individual would like to consider this decision with a family member or trusted person.	
	F) Age Related Vulnerability A customer may be particularly vulnerable as a consequence of the effects aging can have on an individual; this includes potential memory loss, dementia or the potential for the customer to be 'overwhelmed' by a particular situation.	• Be aware of the Power of Attorney requirements where applicable (refer to Horizon Help) • Post Office should not automatically assume that a customer is vulnerable by virtue of their age. We seek to provide appropriate products and services to customers of different ages. However, it is appropriate in some circumstances to explain clearly risks which relate to ageing customers e.g., for end of life planning products. • We aim in our dealings with a customer who we know, or reasonably suspect has a mental capacity limitation, to act sympathetically and positively. • We seek to allow a customer sufficient time to weigh-up the information and explanations we have provided and defer a decision to a later date. We will provide all the information required to enable this. • Where possible we should ask if the individual would like to consider this	Kevin Gilliland / Nick Kennett

POL00401627

		decision with a family member or trusted person.	
	G) Life Event Vulnerability A customer that has or is experiencing a specific adverse 'life event' (for example, redundancy, a bereavement, critical or terminal illness, or a marriage breakdown) could be particularly susceptible to making poor judgements. (Although these triggers may not always have a negative impact on the individual)	• We should aim to treat these customers fairly and with a level of sympathy and positivity. We aim to ensure, throughout our businesses, that when we become aware of these life events we have the ability to respond flexibly and deliver an outcome that is appropriate.	Kevin Gilliland / Nick Kennett
	H) Financial Difficulties Customers that are in financial difficulties (for instance high levels of debt or low levels of income) may be particularly vulnerable to financial detriment.	• Be conscious of customers in financial difficulties when designing or introducing products and services that require a regular financial commitment • Be able to manage expectations e.g., declines or alternate payment methods if applying for a product or service • Where feasible signpost Money Advice Service, Citizen's Advice Bureau, Pensions Advisory Service and/or other similar independent advice/helplines	Kevin Gilliland / Nick Kennett

3. Where to go for help

3.1. Additional Policies

This policy is one of a set of policies. The full set of policies can be found at:

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

3.2. How to raise a concern

Any Post Office employee who is concerned about the application of this policy should:

- Discuss the matter fully with their Line Manager; or,
- Report their concerns to the policy owner.
  If you wish to do this anonymously you should contact the 'Speak Up' line on GRO .

3.3. Who to contact for more information

If you need further information about this policy, please contact Tom Weschler or Jonathan Hill

3.4. Company Details

Post Office Limited registered in England and Wales. Registered numbers 2154540. Registered Office: Finsbury Dials, 20 Finsbury Street, London EC2Y 9AQ.

Post Office Limited is authorised and regulated by Her Majesty's Revenue and Customs (HMRC), REF 12137104. Its Information Commissioners Office registration number is Z4866081.

Version Control

Date	Version	Updated by	Change Details
July 2017	Draft 0.1	Jonathan Hill / Paul Beaumont	1st draft in revised template
11th July 2017	Draft 0.2.1	Jonathan Hill / Paul Beaumont	2nd draft in revised template
26 Sep 2017	Final 1.0	Paul Beaumont	Approved by ARC on 25/9/2017

6.2 Procurement Compliance Reporting

Author: Barbara Brannon Sponsor: Al Cameron Meeting Date: 10 July 2018

Executive Summary

Context

As a business in receipt of public funds POL is bound by the Public Contract Regulations (2015). PCR 2015 oblige POL to behave in a fair, objective & transparent way when contracting with 3rd party suppliers. Additionally, set procedures must be followed for spend above £25k and £181,302 (total contract value, increased from £164,500 in 2018).

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

The PCR Compliance Register allows for the tracking of breaches to PCR regulations at the Post Office and internal governance processes. One aim of collating this information is to drive improvement in awareness and compliance behaviour across the organisation. The second and primary aim is to work with GE and Business Units to commence commercial reviews in a more timely way ensuring POL obtains value, commercial and contractual flexibility fitting the requirements and business strategy of the organisation.

Questions addressed in this paper

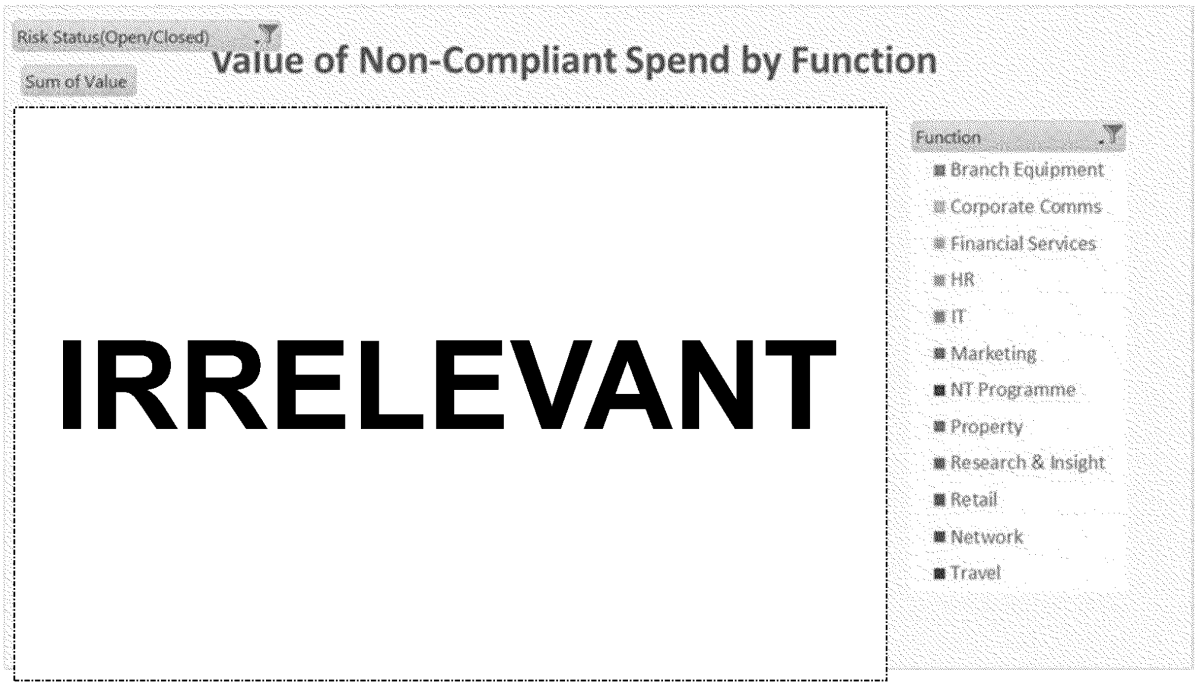
1. *How many and what types of procurement non-compliance have occurred in the past quarter?*
   Since the last RCC report in March there have been a total of 15 non-compliant incidents with a total value of IRRELEVANT With the exception of 2 software related items all material [>£164k] items were included in the pipeline of pending non-compliance supplied to the RCC in March.

2. *What are we doing about it?*

   In the past quarter, while we have added IRRELEVANT we have also resolved IRRELEVANT within the quarter, with only a short term contract extension required and some longer term risk positions resolved notably for IRRELEVANT We have reviewed and adjusted forecast spend data against actuals resulting in a small increase in risk exposure overall. Our overall value has therefore risen from £IRRELEVANT in March to IRRELEVANT in July.

Open non-compliant awards since January 2017 are outlined below:

Function	**March - Sum of Value**	**July - Sum of Value**
Branch Equipment	IRRELEVANT	
Corporate Comms		
Financial Services		
HR		
IT		
Marketing		
NT Programme		
Property		
Research & Insight		
Retail		
Network		
Travel		
Grand Total		



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

4. *Why are these incidents occurring, and what can be done about it?*

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

a) Low value, time constrained or highly sensitive/specialist engagements are common. For example, the Board have requested a number of expedited reviews since the New Year on a short turn-around time.
b) Large commercial arrangements cannot often be easily competed or unravelled without operational impact, and re-procurement may be subject to a pending evolution of a supporting Business Strategy.
c) The contractual arrangements may pre-date PCR 2015 regulations or the contract novated during separation from RMG, automatically becoming non-compliant at the renewal point. Non-compliant awards are frequently made on a tactical basis to extend contractual services while public tender processes are executed.

d) Delays to public sector panels of suppliers becoming available. The Post office makes extensive use of this low cost route to market and new/refreshed panels are subject to frequent delays from Crown Commercial Services. Single interim extensions [of periods under 12 months] while tender processes are run are considered to be low risk legally.
e) Changes in scope or value over the term of a contract may render the extension or renewal of services non-compliant. Material changes to the scope of a contract may render the whole contract non-compliant.
f) Disregard for, or lack of understanding of the regulations.

5. *Why are we receiving this report?*

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

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

   A full list is appended at Appendix B. Since the last RCC in March 2018, two items have been added, only one of which is material and has been the subject of a paper to GE. The first, for branch design activity has been competitively procured under threshold but is expected to breach threshold over the term. The second is for a one year non-compliant extension to our Payments provider to complete a technology upgrade programme. Tender preparation for the new contract term is already underway.

Conclusion

Non-compliant awards of contracts are already subject to extensive internal governance, legal and risk review, explicit GE and Board approval where value/risks reach a minimum threshold.

The YTD non-compliance value is high at IRRELEVANT *the majority of which are interim extensions while procurement processes are run and to allow for operational migration risk to be mitigated. Individually, all large value non-compliant contracts have been* *reviewed by appropriate Post Office governance forums with agreement on next steps and actions towards remediation allocated where appropriate.*

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

Input Sought

Review and note content only.

The Appendix

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

A full explanation of the individual compliance breaches for direct awards over £181k [previously £164k] threshold is attached in Appendix A. Each entry details the nature of, and the value of the breach.

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

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

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

All contracts entered into during this period were compliant with internal governance processes on contract and commercial review. All were for awards of between £0 and £4,000,000.

3. *Why were the approvals given?*

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

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

There were no unapproved, material breaches during this period.

5. Describe the causes of non-compliance to PCR regulations

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

a) Low value, time constrained or highly sensitive/specialist engagements are common. For example, the Board have requested a number of expedited reviews since the New Year on a short turn-around time.
b) Large commercial arrangements cannot often be easily competed or unravelled without operational impact, and re-procurement may be subject to a pending evolution of a supporting Business Strategy.

c) The contractual arrangements may pre-date PCR 2015 regulations or the contract novated during separation from RMG, automatically becoming non-compliant at the renewal point. Non-compliant awards are frequently made on a tactical basis to extend contractual services while public tender processes are executed.
d) Delays to public sector panels of suppliers becoming available. The Post office makes extensive use of this low cost route to market and new/refreshed panels are subject to frequent delays from Crown Commercial Services.
e) Changes in scope over the term of a contract may render the extension or renewal of services non-compliant. Material changes to the scope of a contract may render the whole contract non-compliant.
f) Disregard for, or lack of understanding of the regulations.

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

a) A forward view of material contracts falling under each Business Unit is currently prepared by the relevant Procurement Manager for discussions with their key stakeholders. The maturity of this look ahead view does vary currently and is a high priority activity within the team.
b) Sourcing options papers are prepared for review by contract managers and key stakeholders [risk, legal, security] with routes to market agreed. In many cases these are dependent on evolving business and operating model strategies and the Procurement team are now actively involved with some units helping to advise as thinking evolves.
c) Where a non-compliant award is proposed due to time pressure, Procurement are actively working on long term mitigation with awards made on an interim basis to meet urgent operational needs.
d) Each RCC member will now receive a regular report on compliance within their business unit[s].
e) A new Risk & Governance process requires a Risk Exception report to be created for non-compliant direct awards with SLT or GE sign off.
f) All Professional Services engagements must be approved in writing in advance by the COO. A compliant panel of preferred consulting partners has been appointed and proposed engagements outside of this panel are subject to additional review and challenge.
g) Procurement will now provide training as part of the revised Induction process for new staff. Training packs are being updated for existing staff and made available on the Intranet and ad hoc training sessions for interested Business Units are being run.
h) A new Intranet site has been launched for Procurement to improve visibility of process, regulation, and the panels of approved compliant suppliers available to POL business units.

i) A revised POL Procurement Policy is being drafted giving more granular guidance.
j) Using Crown Commercial Services frameworks, panels of Preferred Suppliers are being refreshed and updated across a wide range of spend categories to reduce time to market, improve compliance and greatly improve commercial outcomes and legal risk.
k) A planned change to operational systems will, once live, give Procurement earlier visibility of potential compliance issues eg: contractual value thresholds.

APPENDIX A : RISK LOG - OPEN ITEMS OVER > £164K

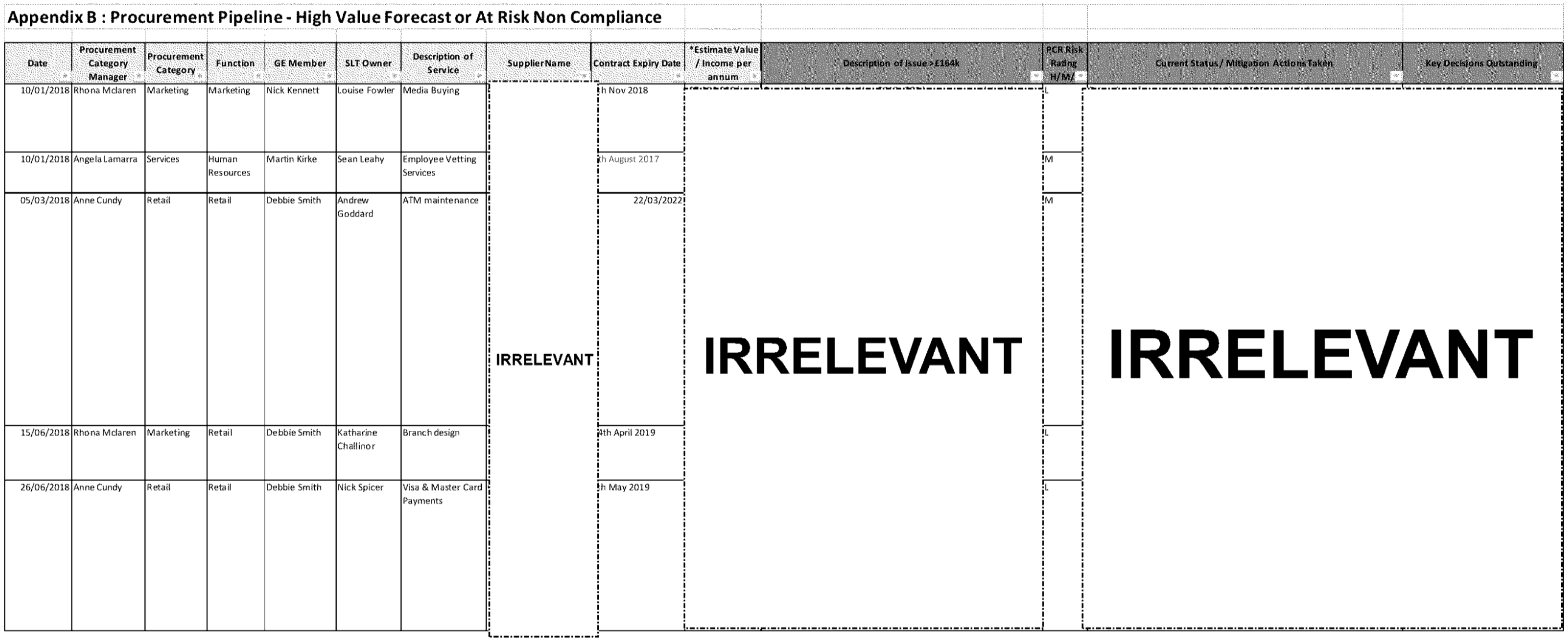
Incident Ref No	Date	Category Manager	Procurement Category	Function	GE Member	Value/ Income	Supplier Name	Breach Type 1 - PCR Threshold	Event (what happened) ONLY FOR £25K>	Actions Taken ONLY FOR £25K>	Further Planned Actions ONLY FOR £25K>
	15.02.2017	Angela Lamarra	Comms, R&I & PR	Corporate Comms	Mark Davies	IRRELEVANT		PCR - >£164.5k	IRRELEVANT		
2017/0009	21 March 2017	Nicola Sams	Comms, R&I & PR	Research & Insight	Paula Vennells			PCR - >£164.5k			
2017/0013	23 March 2017	Angela Lamarra	Professional Services	HR	Martin Kirke			PCR - >£164.5k			
2017/0019	01 June 2017	Antony Ray	Professional Services	HR	Martin Kirke			PCR - >£164.5k			
2017/0036	30th October 2017	Antony Ray	Professional Services	Financial Services	Owen Woodley			PCR - >£164.5k			
2017/0038	01 January 2018	William Porter	Property	Property	Alisdair Cameron			PCR - >£164.5k			

APPENDIX A : RISK LOG - OPEN ITEMS OVER > £164K

Incident Ref No	Date	Category Manager	Procurement Category	Function	GE Member	Value/ Income	Supplier Name	Breach Type 1 - PCR Threshold	Event (what happened) ONLY FOR £25K>	Actions Taken ONLY FOR £25K>	Further Planned Actions ONLY FOR £25K>
2017/0041	10 January 2018	Angela Lamarra	Travel	Travel	Alisdair Cameron	IRRELEVANT		PCR - >£164.5k	IRRELEVANT		
2017/0042	10 January 2018	Angela Lamarra	Professional Services	HR	Martin Kirke			PCR - >£164.5k			
2017/0044	10th January 2018	Shahab Hasan	IT Software	IT	Rob Houghton			PCR - >£164.5k			
2017/0048	23 April 2018	Angela Lamarra	Comms, R&I & PR	Corporate Comms	Mark Davies			PCR - >£164.5k			
2017/0049	23 April 2018	Antony Ray	Comms, R&I & PR	Corporate Comms	Mark Davies			PCR - >£164.5k			
2017/0050	23rd April 2018	Rhona Mclaren	Marketing	Marketing	Owen Woodley			PCR - >£164.5k			
2017/0051	23rd April 2018	Rhona Mclaren	Marketing	Marketing	Owen Woodley			PCR - >£164.5k			

APPENDIX A : RISK LOG - OPEN ITEMS OVER > £164K

Incident Ref No	Date	Category Manager	Procurement Category	Function	GE Member	Value/ Income	Supplier Name	Breach Type 1 - PCR Threshold	Event (what happened) ONLY FOR £25K>	Actions Taken ONLY FOR £25K>	Further Planned Actions ONLY FOR £25K>
2017/0052	23rd April 2018	Rhona Mclaren	Marketing	Marketing	Owen Woodley	IRRELEVANT		PCR - >£164.5k	IRRELEVANT		
2017/0057	04 July 2018	Kelly Snares	IT Software	Marketing	Owen Woodley			PCR - >£164.5k			
2017/0059	04 July 2018	Kelly Snares	IT Software	Marketing	Owen Woodley			PCR - >£164.5k			
2017/0057	08 May 2018	Anne Cundy		Retail	Debbie Smith			PCR - >£164.5k			



Appendix B : Procurement Pipeline - High Value Forecast or At Risk Non Compliance

Date	Procurement Category Manager	Procurement Category	Function	GE Member	SLT Owner	Description of Service	Supplier Name	Contract Expiry Date	*Estimate Value / Income per annum	Description of Issue >£164k	PCR Risk Rating H/M/	Current Status / Mitigation Actions Taken	Key Decisions Outstanding
10/01/2018	Rhona Mclaren	Marketing	Marketing	Nick Kennett	Louise Fowler	Media Buying	IRRELEVANT	h Nov 2018		IRRELEVANT	L	IRRELEVANT	
10/01/2018	Angela Lamarra	Services	Human Resources	Martin Kirke	Sean Leahy	Employee Vetting Services		h August 2017			M		
05/03/2018	Anne Cundy	Retail	Retail	Debbie Smith	Andrew Goddard	ATM maintenance		22/03/2022			M		
15/06/2018	Rhona Mclaren	Marketing	Retail	Debbie Smith	Katharine Challinor	Branch design		4th April 2019			L		
26/06/2018	Anne Cundy	Retail	Retail	Debbie Smith	Nick Spicer	Visa & Master Card Payments		h May 2019			L		

POST OFFICE
RISK AND COMPLIANCE COMMITTEE

PCI Compliance Status Update.

Authors: David Meldrum/Ehtsham Ali Sponsor: Rob Houghton Meeting date: 10 July 2018

Executive Summary

Context

As reported at the last meeting, Post Office (PO) have not yet achieved a Report on Compliance (RoC) from our external qualified security assessor (QSA) proving our compliance to the Payment Card Industry-Data Security Standard (PCI-DSS). Although there has been solid progress, PO still have a significant amount of work to do. The existing RoC expired on 28th December 2017 and we have continued to share our remediation plans with Global Payments (GP), our acquirer, who has indicated general support for our plans and have chosen not to implement any challenges to date. We continue to work with the QSA, and our stakeholders, to initiate a more committed and robust regime of compliance.

Questions this paper addresses

1. Why PCI-DSS is important to the PO business?
2. What challenges are faced with the current audit and the risks associated with delay/failure to receive a RoC?
3. What actions are PO taking?
4. Longer term options as the impacts increase?

Conclusion

- PCI-DSS certification IRRELEVANT PO's ability to evidence continuous work to support PCI-DSS accreditation is essential.
- We have a number of QSA audit non-compliances, and a failure to remediate these could result in some sanctions from our Clients and Partners.
- We have identified 155 remediation activities (96 complete to date) that are being tracked to complete by October 2018. Current dialogue with the QSA, Partners and Clients indicate the risk of sanctions, in the near term, is limited.
- We are initiating an investment in a strategic PCI-DSS solution to resolve the ever increasing challenge of PCI-DSS.

Input Sought

RCC is requested to note this paper and in particularly acknowledge support for a more strategic approach to PCI-DSS compliance subject to PO adequately scoping such work with the QSA and GP accepting this to run alongside the continuous completion of audit actions.

Report

Why PCI-DSS is important to the PO business?

1. PCI-DSS applies to companies of any size that accept or process any card payments data. PO need to host card data securely with the goal of protecting our customer's data.

2. There IRRELEVANT IRRELEVANT This is particularly relevant to the Banking Framework.

3. We have a IRRELEVANT in the Banking Framework. We are in the process of undertaking an external audit of the Banking Framework, the scope is with the banks for review, so we expect it to become clear we are not fully PCI-DSS compliant.

Challenges faced with the current audit and the risks associated with delay/failure to receive a RoC?

4. Recent QSA audits in the early part of 2018 indicated that there were a total of 155 PCI-DSS remediation activities required across the estates managed by ComputaCenter and Fujitsu.

5. The Banks IRRELEVANT IRRELEVANT

6. Although we do not have visibility of any potential charges that GP may levy against us for PCI-DSS non-compliance, we have been informed by our QSA that there are a number of formal steps before fines could be levied.

7. Current dialogue with our acquiring bank is positive and we do not yet feel any intention from GP to notify us of their intention to begin the process to levy fines. Providing it is clearly demonstrated that PO is managing the security of the PCI environment and has a commitment to resolving the PCI compliance issues while working closely with an external PCI QSA, then the bank will generally be comfortable and will not issue any fines.

What actions are PO taking?

8. In order to expedite the completion of all identified non-compliances and the remediation of the outstanding control items; PO are doing the following:

   a. Established daily and weekly progress meetings with Computacenter and Fujitsu respectively, working with them in addressing the gaps identified.

   b. Working with both partners to ensure they design and implement the controls or compensating controls to ensure compliance. Providing rigour and challenge to timescales being presented.

9. There are a number of CR's which are being challenged by our supplier Computacenter and several legal letters have been exchanged on who is liable for cost of PCI – DSS compliance.

10. Re-established a PCI Steering Committee with a focused attendee list and senior business representation to drive forward the strategic solutions and keep the business abreast of the progress made.

11. The proposed technical solutions will need to be applied across our entire estate before the QSA can start their assessment and accordingly the Steering Group has agreed with QSA's recommendation to recommence the audit post completion of the remedial actions.

12. Our QSA has confirmed that our environment is locked down and has no Data or IT security exposures. The branch terminals are running on a dedicated isolated network within Post Office branches. All data, including payment card data is sent from the branch terminals to the Fujitsu data centre over a dedicated network connection and protected with strong encryption.

Longer term options as the impacts increase?

13. The PO PCI-DSS estate is increasing over time (Customer Hub and Panther), although these will be covered by separate certifications, not linked with our current PCI-DSS audit.

14. Customer Hub has successfully been launched and we have successfully attained PCI Certification.

15. A robust strategic approach needs to be in place to align us with the other industry retailers, where PO do not store, process or transmit card data.

16. This approach will require investment and time to implement. Nicholas Spicer and his team within Payment Services are compiling a business case for a possible solution.

17. We will establish a dedicated programme of work to progress the longer term strategic solution that reduces our exposure on relying on our suppliers to maintain our PCI-DSS certification.

POST OFFICE
RISK AND COMPLIANCE COMMITTEE

PCI-DSS Compliance Status Report.

Authors: David Meldrum / Ehtsham Ali   Sponsor: Rob Houghton   Meeting date: 10 July 2018

Executive Summary

Context

As reported at the last meeting, Post Office (PO) are without a Report on Compliance (RoC) from external qualified security assessors (QSA) proving our compliance to the Payment Card Industry-Data Security Standard (PCI-DSS). There has been progress, however PO still do not have a confirmed date when we will be in receipt of our RoC.

The existing RoC expired on 28th December 2017. We have continued to share our remediation plans with Global Payments (GP) our acquirer. Whilst GP could levy penalties against PO, to date, they have not chosen to take this action and there would be extensive dialogue to indicate their intention.

Questions this paper addresses

- Why PCI-DSS is important to the PO business?
- Challenges faced with the current audit and the risks associated with delay/failure to receive a RoC?
- What actions are PO taking?
- Longer term options as the impacts increase?

Conclusion

1. PCI-DSS certification is important to PO as it is a requirement in contracts with Clients and Partners. This has wide reaching impact not only for taking card payments in branch but also for the Banking Framework business.
2. There is no evidence that we would not be able to take card payments and trade without the certification. However, this could impact our ability to meet the North Star strategy to deliver IRRELEVANT profit (grow our business and maximise profits) as winning new business may require PCI-DSS certification as a pre-requisite and our IRRELEVANT IRRELEVANT
3. We have established that remediation activities are being tracked to be completed by October 2018. Of our suppliers who are expected to aid PO in gaining compliance, there are daily progress meetings with Computacenter and twice a week with Fujitsu to ensure they remain on track with the BAU remediation actions.

4. We have set up a programme of work to deliver the strategic solution for PCI-DSS going forwards. This would seek to exclude PO from handling, processing or transmitting card data, and will reduce our dependency on our suppliers to achieve PCI-DSS compliance.

Input Sought

RCC is requested to note this paper.

Report

Why PCI-DSS is important to the PO business?

5. PCI-DSS applies to companies of any size that accept or process any card payments data. PO need to host card data securely with the goal of protecting our customer's data.

6. There is a requirement within many of our contracts with Clients and Partners that PO are PCI-DSS compliant. This is particularly relevant to the Banking Framework.

Challenges faced with the current audit and the risks associated with delay/failure to receive a RoC?

7. We have a IRRELEVANT in the Banking Framework. Banks are IRRELEVANT IRRELEVANT

8. We in the process of undertaking an external audit of the Banking Framework, the scope is with the banks for review, so we expect it to become clear we are not fully PCI-DSS compliant.

9. The Banks IRRELEVANT

IRRELEVANT

10. Although we do not have visibility of any potential charges that GP may levy against us for PCI-DSS non-compliance, we have had to pay higher transactions fees in the past when PO were unable to take contactless payments. In this instance Mastercard Integrity fines, which was 2IRRELEVANT points (minimum charge of IRRELEVANT) of the face value of every MasterCard transaction. That equated to IRRELEVANTn p.a. but if it included Visa it would have been over IRRELEVANT p.a. in higher charges. We have been informed by our QSA that there are a number of steps before fines are issued, with prolonged dialogue with our acquiring bank whereby they notify us of their intention. Each bank has a different approach depending on their risk appetite. Providing it is clearly demonstrated that the organisation is managing the security of the PCI environment and has a commitment to resolving the PCI compliance issues while working closely with an external PCI QSA, then the bank will generally be comfortable. Prior to issuing fines the bank will generally warn the organisation and issue a deadline date for meeting compliance which if not met, may result in fines. To date GP have not made any mention of additional charges or fines due to non-compliance with PCI.

11. There are a number CR's which are being challenged by our supplier (Computacenter) and several legal letters have been exchanged on who is liable for cost, the proposed technical solution will need to be applied across our entire network before the QSA can start their assessment.

12. To put the issues identified by the QSA into context, we believe that our environment is very locked down and has no Data or IT security exposures. The branch terminals are running on a dedicated isolated network within Post Office

branches. All data, including payment card data is sent from the branch terminals to the Fujitsu data centre over a dedicated network connection and protected with strong encryption. The issues noted are relate to compliance to PCI standards.

What actions are PO taking?

13. In order to expedite the completion of all identified non-compliances and the remediation of the 4 outstanding issues, PO are doing the following:

    a. Established daily progress meetings Computacenter, working with them in addressing the gaps identified.

    b. We have appointed a full time project manager to ensure all issues are addressed in a timely fashion.

    c. PO have been working with CC to ensure they design and implement the controls or compensating controls ensure compliance. Providing rigour and challenge to timescales being presented.

14. -Re-established a PCI Steer-Co with a focused attendee list and senior business representation to drive forward the strategic solutions and keep the business abreast of the progress made.

15. -Clarified the position regarding PODG being in scope of our assessment with our suppliers and QSA, agreed that this will be proposed to be de-scoped from the PCI audit through discussions with our acquiring bank which our QSA will support.

Longer term options as the impacts increase?

16. The PO PCI-DSS estate is increasing over time (Customer Hub and Panther), although these will be covered by separate certifications, not linked with our current PCI-DSS audit. Customer Hub has successfully been launched and they have attained their own PCI Certification.

17. A robust strategic approach needs to be in place to align us with the other industry retailers, where PO do not store, process of transmit card data. This approach will require investment and time to implement. Nicholas Spicer and his team within Payment Services are compiling a business case for a possible solution.

18. Established a dedicated programme of work to progress the longer term strategic solution that reduces our exposure on relying on our suppliers to maintain our PCI-DSS certification.

Gifts & Hospitality Annual Review 2017-18

Author: Sally Smith Sponsor: Jane MacLeod Meeting Date: July 2018

Executive Summary

Context

As part of our annual Anti-Bribery and Anti-Corruption (ABC) obligations, this paper provides an overview of the Gifts & Hospitality reporting for the period 2017-18.

Questions addressed in this paper

- What issues have been highlighted based upon the review?
- What actions need to be undertaken to address any issues?

Conclusion

1. Whilst there have been breaches relating to adherence to the policy, we have not identified any instances indicative of Bribery or Corruption.

2. Quality and quantity of gifts and hospitality reporting has greatly improved compared to the same period last year, although there is still more that needs to be done to change the culture in relation to the correct reporting and approval.

Input Sought

The R&CC is asked to review this report and consider whether any further actions should be taken to further improve gifts and hospitality reporting.

The Report

Summary of ABC activities relating to Gifts & Hospitality reporting 2017-18

1. The new reporting tool was delivered in August 2017, and an FAQ area has been added to the reporting tool covering common questions and reporting issues
2. Quarterly reporting to all GE members commenced from October 2018, summarising overall Post Office reporting and highlighting any breaches or concerns for each GE's business area.
3. There have been 3 communications issued relating specifically to Gifts and Hospitality reporting.
4. Enhanced mandatory ABC training was delivered in September 2017 and this is now tracked from weekly Success Factors reports by HR Directors.

Summary of Gifts & Hospitality received and offered 2017-18

5. Analysis of the 2017-18 Gifts & Hospitality Register has highlighted that the quality of submissions made in this period compared to the same period last year has greatly improved (please see Appendix A & B for data):
    - In 2016/17 there were 17 gift reports totalling £230 and 128 hospitality reports totalling £5475.55
    - In 2017/18 there were 27 gift reports totalling £1521 and 195 hospitality reports totalling £33,673.07
6. Whilst an improvement has been seen, it is believed that there is still significant under-reporting, particularly relating to gifts and declined offers.
7. In the reporting period, the following common breaches were identified:
    - A number of instances where employees have accepted gifts of cash or cash equivalent (e.g. gift cards). Whilst the members of staff reported these, cash gifts are against policy and should have been returned to the customer. These instances were reported to relevant line managers after the report was submitted to ensure that the gifts were returned and further guidance given to staff members.
    - There have been a number of instances where offers of hospitality have been submitted and approved retrospectively. Again, guidance has been given to relevant line managers and individuals.
    - A trend has been identified where submissions are being reported with the title description "Hospitality" rather than, for example, "dinner with x". The title field of the reporting tool has been amended to assist users to correctly report submissions.
8. A review of the external companies that have offered hospitality to Post Office in 2017/18 has not identified any significant issues, and the top 6 are detailed below:

External Party Name	**Volume**	**People**	**Value**
FRES (First Rate Exchange Services)	22	24	£ 2,580.00
Kings Security	6	6	£ 1,780.00
CMS LLP	8	31	£ 1,200.00
Womble Bond Dickinson	6	22	£ 1,130.00
Chemistry Club	7	16	£ 540.00
Bank of Ireland	6	7	£ 369.22

Planned actions to address issues:

9. The following activities are planned to improve the quality and effectiveness of gifts and hospitality reporting and approval:
   - ABC training is scheduled for the end of July 2018 and the content has been amended to help address common failings identified during 2017-18 and make the reporting and approval requirements easier to understand
   - A summer reminder communication is scheduled to be issued during July, with further communication and awareness activity planned throughout the year
   - Financial Crime will continue to monitor gifts and hospitality reporting and feedback to individuals and line management

Appendix A – Gifts and Hospitality for 2017/18

The below tables sets out all gifts and hospitality offered and received by GE member:

Pre-Introduction of the Gifts and Hospitality Reporting Tool:

1st April 2017-7th August 2017	Gift		Hospitality		Total	
Business Team	**Volume**	**Value**	**Volume**	**Value**	**Volume**	**Value**
Communication, Brand & Corporate Affairs	0	£0.00	0	£0.00	0	£0.00
Finance and Operations	0	£0.00	4	£320.00	4	£320.00
Financial Services and Telecoms	0	£0.00	13	£2,348.00	13	£2,348.00
HR	1	£0.00	0	£0.00	1	£0.00
IT	1	£60.00	1	£400.00	2	£460.00
Legal, Risk and Governance	0	£0.00	12	£2,827.00	12	£2,827.00
Retail	0	£0.00	8	£1,010.00	8	£1,010.00
Strategy	0	£0.00	0	£0.00	0	£0.00
Grand Totals	**2**	**£60.00**	**38**	**£6,905.00**	**40**	**£6,965.00**

Post Introduction of the Gifts and Hospitality Reporting Tool:

8th August 17-31st March 18	Gift		Hospitality		Total	
Business Team	**Volume**	**Value**	**Volume**	**Value**	**Volume**	**Value**
Communication, Brand & Corporate Affairs	1	£35.00	5	£1,534.00	6	£1,569.00
Finance and Operations	8	£511.00	19	£5,662.00	27	£6,173.00
Financial Services and Telecoms	6	£180.00	46	£5,223.07	52	£5,403.07
HR	0	£0.00	8	£625.00	8	£625.00
IT	0	£0.00	5	£399.00	5	£399.00
Legal, Risk and Governance	3	£130.00	56	£11,338.00	59	£11,468.00
Retail	7	£605.00	17	£1,887.00	24	£2,492.00
Strategy	0	£0.00	1	£100.00	1	£100.00
Grand Totals	**25**	**£ 1,461**	**157**	**£ 26,768.07**	**182**	**£ 28,229.07**

Appendix B – Gifts and Hospitality for 2016/17

The below tables sets out all gifts and hospitality reported for the 2016/17 financial year:

Gifts		**Hospitality**	
Total volume	17	*Total volume*	128
Total value	£230.00	*Total value*	£5,475.55
Amount without value recorded	7	*Amount without value recorded*	100
Amount with value recorded	10	*Amount with value recorded*	28
Declined	1	*Declined*	14
Value within policy amount (<£200)	10	*Value within policy amount (<£100)*	23
Value above policy amount (>£200)	0	*Value above recommended policy amount (>£100)*	5 (all authorised in line with Policy)
Policy Breaches	1 – acceptance of £100 cash	*Policy breaches*	0

As reported last year, due to the inconsistencies in the information captured data could not be properly analysed and due to structural changes within Post Office during the 2016/17 financial year it is not possible to compare the separate business areas.

Anti-Bribery & Anti-Corruption Policy

Author: Sally Smith Sponsor: Jane MacLeod Meeting Date: 10th July 2018

Executive Summary

Context

This paper sets out the updates and revisions to the Anti-Bribery and Anti-Corruption (ABC) Policy as part of the annual review process for the Risk and Compliance Committee to consider and approve.

Questions addressed in this paper

- What changes to the Policy do we propose and why?
- What are the implications of these changes?

Conclusion

1. The ABC Policy has been amended to ensure it reflects industry best practice and provide clarity as to role and responsibilities in relation to the minimum control standards.
2. The updated Policy reflects queries and issues received by the Financial Crime team over the last 12 months.

Input Sought

The R&CC is asked to approve the updated ABC Policy.

The Report

Why do we need to review this Policy?

3. The Policy was last reviewed and approved by the R&CC in July 2017. The terms of the Policy require it be reviewed annually.

What changes to the Policy do we propose and why?

What are the key features that we propose and why?

4. There have been no legislation changes in the past year and no significant amends made to the policy at this annual review.
5. Minor amends have been made in relation to:
   - The location on the Intranet of the Risk Exception process
   - Mandatory ABC training for all staff has been included in the minimum control standards as a key preventative control
   - Gifts and hospitality minimum control standards have been amended to clarify line management and Financial Crime responsibilities in approving, reviewing and monitoring submissions
   - To reflect industry best practice, charity donations risk area has been amended to include sponsorship, with a new control that the relevant GE member approves any cash donations or sponsorship made by Post Office

How did we develop these recommendations?

6. A review of bribery and corruption cases and penalties publicly reported over the last 12 months and cases that the Financial Crime team has been involved in via the Joint Money Laundering Intelligence Taskforce.
7. Policy queries and issues that have arisen over the previous 12 months have been reviewed to ensure that these concerns are addressed. The definitions have been updated to clarify queries and issues raised by key stakeholders.

What are the implications of these changes?

What will we need to do and by when, to implement and embed these Policy changes?

8. No material changes are required to comply with this updated Policy.
9. All employees need to ensure that they accurately report all instances of gifts and hospitality offered and declined using the reporting tool to obtain appropriate approval.
10. Internal communications and training – once the Policy has been approved, there will be a One communication to advise all employees with a link to the updated document and the Gifts and Hospitality Tool on the Post Office Intranet.
11. The Financial Crime Team will continue to provide quarterly reports to Group Executive members.
12. Every six months, as part of the Group Executive declaration the members are required to confirm that the Policy has been correctly applied in their business area.

What will the impact be on our wider business?

13. Increased transparency of the ABC framework and commitment to maintaining visible compliance with the applicable legislation.
14. Reinforcement that the failure to comply with the requirements of ABC Policy by any employee will be regarded as a significant breach impacting on the Post Office's risk and control management environment and may lead to disciplinary action up to and including dismissal and possible prosecution.
15. The Financial Crime Team monitor adherence to the minimum control standards set out in the Policy on an on-going basis through their review of the Gifts and Hospitality Tool and any other reported issues - any control gaps identified are reported to the R&CC as required. Appendix A provides an overview of the assurance checks developed by the Financial Crime team during 2017/18.

What would the impact be of delaying approval?

16. Risk that the group breaches the Bribery Act 2010 by not having up to date policies and procedures to prevent bribery by any person or company who operates on our behalf.
17. Post Office Limited is required to maintain up to date policies to support contractual requirements with clients and suppliers (e.g. MoneyGram and the Partner Banking Framework) and failure to do so may result in a breach of contract, and whilst not material, could have commercial and reputational impacts.
18. Post Office Limited provides Post Office Management Services (POMS) with its policies suite in the form of "Group Policies". POMS is required under its regulatory responsibility to the Financial Conduct Authority to have up to date policies and failure to do so may lead to regulatory sanctions or penalties.

Appendix A - ABC Policy Minimum Control Standards Assurance

The below table shows the residual risk rating from a first and second line of defence perspective for each control type within the currently approved policy as at the Q1 2018/19 review

Risk Description	Control Type	Description of control	Residual risk rating			Control Strength		Q1 Assurance Comments
			L	I	S	1st LoD	2nd LoD	
Failure to ensure that Consultants and Contractors comply with the Group's anti-bribery and corruption policy	Preventative	(a) Training of contractors; (b) Contractual compliance with policies by consultants.	3	3	9	Partially effective	Effective	Weekly report from SF provided to all HR directors for them to follow through with individuals who have not completed mandatory training as required. During checks undertaken by FC in April it was noted that the percentage of completion by contractors was down to 88% and a chaser was sent to the HR Director. Latest completion rates showing improvement to 92%. Weekly monitoring in place. Not all contracts currently include ABC requirements. 1LOD assessed as partially effective as drop in training completion observed during quarter and some contract gaps.
Insufficient controls may lead to the donation of money to an unregistered charity, which could be interpreted as bribery	Preventative	(a) Validate charity via The Charity Commission. (b) Training of all employees	2	2	4	Effective	Partially effective	No mention of the protocol associated with charities in G&H reporting. ABC policy refers to charity donations, and guides user to a web link which opens a page with error and is being fixed. The G&H process doc is currently being updated and ABC training enhanced.
Insufficient controls may lead to the donation of money to an unregistered charity, which could be interpreted as bribery	Detective	(a) Monitoring of Training attempts	2	2	4	Effective	Partially effective	No mention of the protocol associated with charities in G&H reporting. ABC policy refers to charity donations, and guides user to a web link which opens a page with error and is being fixed. The G&H process doc is currently being updated and ABC training enhanced.
The acceptance of hospitality or gifts from third parties could lead to bias or undue influence, or the perception of such, in how individuals	Preventative	(a) G&H approval process (b) ABC Training	2	3	6	Partially effective	Effective	Report sent to all GE in April and summary included in May RCC report. Specific failures called out in May report and FC continue to monitor inbox for non-conformances. Annual training brought forward to July will highlight weaknesses identified throughout year.

Risk Description	Control Type	Description of control	Residual risk rating			Control Strength		Q1 Assurance Comments
			L	I	S	1st LoD	2nd LoD	
exercise their duties and responsibilities.								
Failure to identify employees requesting or receiving something of value from a third party in exchange for providing employment or work opportunities may result in the loss of Group stakeholder support.	Preventative	(a) Review of all employment	2	3	6	Effective	Effective	Employment process is robust. All employees subject to on boarding policy and procedures and employee data held in success factors
Inadequate controls may lead to employees accepting gifts that are not appropriate, proportionate or within policy resulting in reputational damage or criminal prosecution.	Preventative	(a) G&H reporting tool with clear process in place to be completed when a colleague receives or offers a gift over the value of £20; (b) LM and GE approval required where appropriate; (c) Prohibit accepting cash or equivalents; (d) Group wide training programme	2	3	6	Partially effective	Effective	Report sent to all GE in April and summary included in May RCC report. Specific failures called out in May report and FC continue to monitor inbox for all non-conformances. Annual training brought forward to July will highlight weaknesses identified throughout year.
Inadequate controls may lead to employees accepting gifts that are not appropriate, proportionate or within policy resulting in reputational damage or criminal prosecution.	Corrective	(a) Corrective action when required.	2	3	6	Partially effective	Effective	FC monitor all reports received and instigate corrective action where required. To date, no instances have required escalation to HR.

Risk Description	Control Type	Description of control	Residual risk rating			Control Strength		Q1 Assurance Comments
			L	I	S	1st LoD	2nd LoD	
Inadequate controls may lead to employees accepting hospitality that are not appropriate, proportionate or within policy.	Preventative	(a) G&H reporting tool with clear process in place to be completed when a colleague receives or offers Hospitality; (b) LM and GE approval required where appropriate; (c) Hospitality must be reasonable, ordinarily below the value of £200; (d) Group wide training programme	3	3	9	Partially effective	Effective	Report sent to all GE in April and summary included in May RCC report. Specific failures called out in May report and FC continue to monitor inbox for all non-conformances. Annual training brought forward to July will highlight weaknesses identified throughout year.
Inadequate controls may lead to employees accepting hospitality that are not appropriate, proportionate or within policy.	Corrective	(a) Corrective action when required.	3	3	9	Partially effective	Effective	FC monitor all reports received and instigate corrective action where required. To date, no instances have required escalation to HR.
Offering facilitation payments, gifts & entertainment, client training programmes, charitable or political donations, ex-gratia payments or legal settlements that are not justifiable or proportionate.	Preventative	(a) Conflicts of Interest policy; (b) G&H reporting tool; (c) Group wide training (d) Group Legal Director approval for ex-gratia payments (e) Group wide training programme	1	4	4	Partially effective	Partially effective	CoI policy was due for renewal Mar 2017. Policy referred to CoSec who are undertaking review and update. On Diary for update end June. Existing policy is available on intranet. Assessed as partially effective as policy is currently out of date.
Employees making or soliciting political donations on behalf of Post Office	Preventative	(a) GE approval (b) Prohibit giving Political donations/Gifts	2	2	4	Effective	Partially effective	G&H process doc states that G&H associated with political parties/ representatives is to be avoided. Comms and awareness improvements needed

Risk Description	Control Type	Description of control	Residual risk rating			Control Strength		Q1 Assurance Comments
			L	I	S	1st LoD	2nd LoD	
Inadequate monitoring may lead to third parties engaging in bribery or corruption while performing services on behalf of the Post Office Group.	Preventative	(a) CFO review of fees paid (b) Review of new/ existing contracts; (c) Conflicts of Interest policy	2	2	4	Effective	Partially effective	Psuite has been agreed and signed off and includes specific ABC clauses. Procurement aware of requirements around lock downs. Assessed as partially effective as lock down is reliant on individuals compliance and there are no system controls.

GROUP POLICIES

Anti-Bribery and Corruption Policy

Version – V2.1

Chief Executive's Endorsement

The Post Office Group is committed to doing things correctly. Our Values and Behaviours represent the conduct we expect. This Policy supports these to help us ensure the highest standards of financial crime prevention, detection and management are maintained.

1. Overview

1.1. Introduction by the Policy Owner

The General Counsel has overall accountability to the Board of Directors for the design and implementation of controls to prevent or deter Bribery and Corruption. Anti-Bribery and Corruption is an agenda items for the Audit and Risk Committee and the Post Office board is updated as required.

1.2. Purpose

This Policy has been established to set the minimum operating standards relating to the management of our Bribery and Corruption risks throughout the Group[1]. It is one of a set of policies which provide a clear risk and governance framework and an effective system of internal control for the management of risk across the Group. Compliance with these policies supports the Group in meeting its business objectives and to balance the needs of shareholders, employees[2] and other stakeholders.

1.3. Core Principles

To offer a bribe is a criminal offence; bribery is an offer, promise, payment, request, or agreement to receive anything of value from any person or entity in order to induce that person to perform their roles improperly.

In order to prevent Bribery and Corruption the governance arrangements described in this Policy are based upon the following core principles:

- The Group is committed to and oversees the implementation of a Policy of zero tolerance, recognising that bribery is contrary to fundamental values of integrity, transparency and accountability and undermines the Group's effectiveness;
- Post Office has devised a robust Policy and associated procedures (set out in this document) which are proportionate to the risks and complexity of the Group;
- A bribery risk assessment is an integral part of our Group's overall and ongoing risk management process;
- Post Office must assess the risk associated with entering into joint ventures, partnerships or contracting arrangements with other entities and must carry out periodic due diligence based on that risk assessment. This includes ensuring that these organisations have policies and procedures which are equivalent to the Group's own procedures;
- The Group undertakes a training and awareness program to ensure employees are aware of the potential risks, how bribery might affect them, what they should do if they are offered a bribe, and the consequences should they be found to have made or received a bribe;
- The interests of Policyholders and other stakeholders are protected by ensuring that excessive powers are not delegated to individuals;

[1] In this Policy "Post Office" and "Group" mean Post Office Limted and Post Office Management Services Limited.

[2] In this Policy "employee" means permanent staff, temporary including agency staff, contractors, consultants and anyone else working for or on behalf of Post Office.

- Decisions taken by management are consistent with the Group's strategic objectives and risk appetite, which are approved by the Board;
- Appropriate conduct is demonstrated in executing the requirements contained within the Policy;
- Every member of staff is responsible for understanding and managing the risk they take on behalf of the Group and for ensuring that they act within accordance to them;
- All employees are required to comply with Group Policies.

1.4. Application

This Policy is applicable to all areas within the Group and defines the minimum standards to control financial loss, customer impact, regulatory breaches and reputational damage in line with the Group's Risk Appetite.

In exceptional circumstances, where risk sits outside of the Group's accepted Risk Appetite a Risk Exception can be granted. F~~or f~~urther information in relation to the risk exception process, together with a template can be found on the Intranet..... ~~please contact the Risk & Assurance team – adnan.killedar~~ GRO ~~or georgina.blair~~ GRO [SS1][SS2]~~.~~

While Post Office does not tolerate events that are criminal in nature and which may give rise to unacceptable and illegal behaviour, it recognises that despite its many endeavours, it is not possible to eliminate all risks of internal and external Bribery and Corruption. As a result Post Office may incur losses, and therefore takes a risk based approach to Bribery and Corruption.

For definitions please see section 3.1.

The risk to the Group in relation to Bribery and Corruption is reviewed by the board on a regular basis.

1.5. Types of Bribery and Corruption Risk

Post Office is exposed to a number of the above risks relating to Bribery or Corruption. These risks include, but are not limited to, the following:

1. **Payment Risks** –for example, facilitation payments, gifts & hospitality, client training programmes, charitable or political donations, ex-gratia payments/ legal settlements. This would also include the offer of sponsorships or grants.
2. **Third Party/Associated Party Risks** –third parties who provide services on behalf of the Post Office Group engaging in bribery or corruption while performing such services. The scope of this could include agency operators within the Post Office network and suppliers procured through the business or through the Procurement Team. Examples of Associated Parties include agents, consultants, suppliers, introducers, and intermediaries.

3. **Employment Risks** –Post Office employees requesting or receiving something of value from a third party in exchange for providing employment or work opportunities at the Post Office or offering or providing work opportunities, paid or unpaid, to Connected Individuals[3], or otherwise using employee connections to improperly obtain business or secure an advantage for Post Office. Employment opportunities (including work experience, secondments, etc.) have a value to the recipient and/or their close family members and may be considered to be bribes if used to improperly obtain or retain business or secure an advantage for Post Office.

4. **Inducement Risks -** Post Office must take reasonable steps to ensure that it, and any person acting on its behalf, does not:
   - Offer, give, solicit or accept an inducement; or
   - Direct or refer any actual or potential business in relation to another person on its own initiative or on the instructions of an associate; if it is likely to conflict to a material extent with any duty that Post Office Management Services owes to its customers in connection with an insurance mediation activity or any duty which such a recipient firm owes to its customers in connection with an insurance mediation activity.

5. **Gifts & Hospitality** –The Group has a process for reporting Gifts & Hospitality (both received and offered) details of this can be found here.

1.6. Legislation

The Group seeks to comply with all relevant UK legal and regulatory requirements including (but not limited to):

- The Bribery Act 2010
- The Criminal Finances Act 2017
- Financial Conduct Authority (FCA) Rules and Guidance (to the extent that these apply – see 1.8 below)

Under the Bribery Act, it is an offence to:

- Directly, or indirectly offer, promise or give a financial or other advantage with the intention of inducing any person to perform a business activity improperly or to reward any person for doing so;
- Request, agree to receive or accept a bribe, i.e. to receive a financial or other advantage with the intention of performing a business activity improperly;
- Bribe a foreign public official;
- Fail to prevent bribery by any person who perform services for or on behalf of a company ("corporate offence").

Post Office is subject to the Bribery Act 2010 (Bribery Act) and could become criminally liable as a result of an act of bribery or corruption by its employees or a third party operating on our behalf.

The Bribery Act has extra-territorial effect which means that the actions of Post Office or a third party operating on our behalf outside of the UK may fall within the scope of the Act. In the context of Post Office, this could apply in scenarios such as where a Post Office contractor or supplier resides outside the UK.

[3] Connected Individuals means those individuals who are known to have close connections to existing or prospective clients or suppliers, Public Officials, Politically Exposed Persons (PEP) or using employees' connections to improperly obtain business or secure an advantage for Post Office.

The Criminal Finances Act also includes a 'failure to prevent' (strict liability) offence on the Group, where failure to prevent criminal facilitation of a tax evasion offence, by a taxpayer, takes place and there are no reasonable procedures put in place to prevent such facilitation, or it cannot show that these procedures would have been unreasonable.

Post Office can be held liable unless it can demonstrate that it has in place "adequate procedures" designed to prevent this type of misconduct. The controls outlined in this Policy, including appendices, assist Post Office in preventing and detecting corrupt conduct and form an essential component of Post Office's adequate procedures.

1.7. FCA Rules

Post Office Limited is an Appointed Representative of the Bank of Ireland and Post Office Management Services Limited (POMS) and is contractually required to comply with certain regulatory requirements. As such the Group as a whole is obliged to ensure there are adequate systems and controls are in place to mitigate Financial Crime risks.

POMS is a directly regulated firm with the FCA is directly exposed to regulatory fines and censure if the FCA determine that the systems and controls associated with this Policy are not effectively implemented.

This Policy contributes to Post Office's compliance with these regulatory and contractual obligations.

2. Risk Appetite and Minimum Control Standards

2.1. Risk Appetite

Risk Appetite is the extent to which the Group will accept that a risk might happen in pursuit of day to day businesses transactions. It therefore defines the boundaries of activity and levels of exposure that the Group are willing and able to tolerate.

The Group takes its legal and regulatory responsibilities seriously and consequently has[4]:

- **Tolerant risk appetite** for Legal and Regulatory risk in those limited circumstances where there are significant conflicting imperatives between conformance and commercial practicality
- **Averse risk appetite** for litigation in relation to high profile cases/issues
- **Averse risk appetite** for ligation in relation to Financial Services matters
- **Averse risk appetite** for not complying with law and regulations or deviation from business' conduct standards for financial crime to occur within any part of the organisation
- **Averse Risk Appetite** in relation to unethical behaviour by our staff.

The Group acknowledges however that in certain scenarios even after extensive controls have been implemented a product or transaction may still sit outside the agreed Risk Appetite. In this situation, a risk exception waiver will be required[5].

2.2. Policy Framework

Post Office has established a suite of financial crime policies and procedures, on a risk sensitive approach which are subject to an annual review. The Policy suite is designed to combat money laundering, terrorist financing, bribery and corruption and adhere to relevant Sanctions regimes. These have been developed to comply with applicable legislation and regulation and covers the following specifically:

- The identification of potential financial crime risks
- On a risk sensitive approach, performing due diligence at on-boarding, periodic basis and payment on third parties who perform services for or on behalf of us.
- Maintaining appropriate records for at least the minimum UK prescribed periods.
- Completing compliance oversight monitoring to test the Group's controls and confirming effectiveness and adherence to financial crime policies.
- Establishing and maintaining Standards for Management Information on Financial Crime. This includes, but is not limited to, record keeping, reporting of suspicious activity and details of staff training.

The Anti-Bribery and Corruption Policy is a key Policy under the Financial Crime Policy framework and should be considered and read in conjunction with the overarching Financial Crime Policy where relevant.

[4] The Risk appetite was agreed by the Groups Board January 2015
[5] For more information in relation to Risk Exception waivers please see section 1.4

2.3. Who Must Comply?

Compliance with this Policy is mandatory for all Post Office employees and applies wherever in the world the Group's business is undertaken. All third parties who do business with the Group, including consultants, suppliers and business and franchise partners, will be required to agree contractually to this Policy with their own equivalent Policy.

Where non-compliance is identified the matter must be referred to the Director of ~~Risk and~~ Compliance and the Group Legal Director. Any investigations will be carried out in accordance with the Investigations Policy. Where is it identified that that an instance of non-compliance is caused through wilful disregard or negligence, this will be treated as a disciplinary offence.

All Post Office employees are required to report any knowledge or suspicions in relation to Bribery or Corruption to Grapevine. As such all business units are required to have a process in place for reporting Bribery or Corruption incidents to Grapevine by telephone on GRO For more information in relation to reporting knowledge or suspicions please see section 3.2.

The next page sets out the minimum control standards that the Group has implemented to control these risks.

2.4. Gifts and Hospitality Tool

The purpose of the Gifts and Hospitality Tool is to make it easy for our employees to accurately record the offering and acceptance of gifts and hospitality throughout the Group. For more information in relation to the tool and how to use this, please see the below links:

The Gifts and Hospitality Tool can be found here.

Instructions upon how to complete the tool can be found here.

The procedure for completing the Gifts and Hospitality Tool can be found here.

2.5. Minimum Control Standards

A minimum control standard is an activity which must be in place in order to manage the risks so they remain within the defined Risk Appetite statements. There must be mechanisms in place within each business unit to demonstrate compliance. The minimum control standards can cover a range of control types, i.e. directive, detective, corrective and preventive which are required to ensure risks are managed to an acceptable level and within the defined Risk Appetite.

The table below sets out the relationships between identified risk and the required minimum control standards in consideration of the stated risk appetite. The subsequent pages define the terms used in greater detail:

Risk Area	**Description of Risk**	**Minimum Control Standards**	**Who is responsible**	**When**
Appointment and Activities of Consultants and Contractors	Failure to ensure that Consultants and Contractors comply with the Group's anti-bribery and corruption policy may lead to criminal prosecution and damage to the Post Office brand or reputation.	Preventative Control: Our contracts require Consultants and Contractors to comply with the Group's anti-bribery and corruption policy. A clause is included within Consultants and Contractors contracts requiring them to comply with the Group's anti-bribery and corruption policy.	Procurement	Ongoing where required
Charity Donations and Sponsorship	Insufficient controls may lead to the donation of money to an unregistered charity, which could be interpreted as bribery and result in reputational damage.	Preventative Control: Where the Group, a team or an individual has selected a particular charity to support, they are required to validate that charity against the Charity Commissions website. More information can be found here. Where a supplier or third party requests that Post Office makes a charitable donation, Post Office ensures that the donation	All employees	Ongoing

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
		is not linked to any business or services provided to or by that supplier or third party. Any cash donations or sponsorship should be approved by the relevant GE member to ensure appropriateness[SS3] Post Office has a Group wide training programme to ensure that all customer facing staff, back office staff and contractors receive adequate training. Staff and contractors are required to complete training within 30 days of joining Post Office and annually[SS4]. Outsource providers, clients & suppliers must maintain records to evidence that staff have received adequate and regular training. Detective Controls: Pass rate and number of test attempts is monitored to identify risk areas and any additional training or guidance required.	All employees GE are responsible for approval of cash donations and sponsorship Human Resources is responsible for any incidents where further action is required and ensuring completion of mandatory training Financial Crime Team is responsible for reviewing training effectiveness	Ongoing
Conflicts of Interest	The acceptance of hospitality or gifts from third	Preventative Control:	All employees	Ongoing

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
	parties could lead to bias or undue influence, or the perception of such, in how individuals exercise their duties and responsibilities.	The Group operates a procedure to ensure Gifts and Hospitality may not be offered or accepted where they could bias or influence how individuals exercise their duties and responsibilities. All employees are made aware of and are expected to comply with the gifts and hospitality procedures.		
Employment Risks	Failure to identify employees requesting or receiving something of value from a third party in exchange for providing employment or work opportunities may result in the loss of Group stakeholder support.	Preventative Control: Any form of employment or work opportunities (paid or unpaid) must be reviewed and approved prior to employment.	All employees	Ongoing
Gifts	Inadequate controls may lead to employees accepting gifts that are not appropriate, proportionate or within policy resulting in reputational damage or criminal prosecution.	Preventative Control: All employees must report correctly ~~any~~ all gifts ~~or hospitality~~ of £20 and over which they receive or offer using the Gifts & Hospitality tool, whether accepted or declined. No employee may accept cash (or cash equivalent) gifts.	Each employee is responsible for ensuring that all gifts offered or received are recorded. Line managers are responsible for ensuring the gift complies with	Ongoing Ongoing Ongoing

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
		Post Office has a Group wide training programme to ensure that all customer facing staff, back office staff and contractors receive adequate training. Staff and contractors are required to complete training within 30 days of joining Post Office and annually. Corrective Control: Where an issue is identified, the reason for this is reviewed and action is taken. Action may include~~s~~ disciplinary and dismissal.	policy and is reasonable and for approving or declining the acceptance of a gift[SS5] Group Executive are~~is~~ responsible for approving or declining any offers over £100 Financial Crime Team is responsible for ~~reviewing~~ reviewing and monitoring the Gifts and Hospitality register. Human Resources is responsible for ~~reviewing~~ any incidents where further action is required and ensuring completion of mandatory training	Ongoing Ongoing
Hospitality	Inadequate controls may lead to employees accepting hospitality that is not appropriate, proportionate or within policy resulting in reputational damage or criminal prosecution.	Preventative Control: All employees must report correctly any ~~gifts or~~ hospitality which they receive or offer using the Gifts & Hospitality tool, whether accepted or declined[SS6]. Before accepting or giving hospitality an employee must receive written approval from their line manager.	Each employee is responsible for ensuring that all hospitality offered/received are recorded Line managers are responsible for ensuring the gift complies with policy and is reasonable and for approving or	Ongoing Ongoing Ongoing

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
		The hospitality must be reasonable (not lavish or extravagant), proportionate to its purpose and must ordinarily be below £200 per person in value. Post Office has a Group wide training programme to ensure that all customer facing staff, back office staff and contractors receive adequate training. Staff and contractors are required to complete training within 30 days of joining Post Office and annually.	declining the acceptance of hospitality Group Executive are~~is~~ responsible for the approving or declining of any offers of hospitality over £200 Financial Crime Team is responsible for reviewing and monitoring the Gifts and Hospitality register Human Resources is responsible for ~~reviewing~~ any incidents where further action is required and ensuring completion of mandatory training	Ongoing Ongoing
Payment Risks	Offering facilitation payments, gifts & entertainment, client training programmes, charitable or political donations, ex-gratia payments or legal settlements that are not justifiable or proportionate may result in reputational damage or criminal prosecution.	Preventative Control: All employees are required to comply with the conflicts of interest policy which can be found here. All employees are required to comply with the Gifts and Hospitality procedure which can be found here. The acceptance of discounted or complimentary training courses which would usually incur a cost are classified as Gifts and	Each employee is responsible for ensuring that all hospitality and gifts offered or received are recorded Line managers are responsible for approving or declining the acceptance of a gift or hospitality. Group Executive are~~is~~ responsible for the approving or declining of	Ongoing Ongoing Ongoing

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
		Hospitality and employees are required to report these using the Gifts & Hospitality Tool. The payment of ex-gratia payments or legal settlements are strictly controlled and must be submitted to the Group Legal Director for approval. Post Office has a Group wide training programme to ensure that all customer facing staff, back office staff and contractors receive adequate training. Staff and contractors are required to complete training within 30 days of joining Post Office and annually.	any offers of gifts or hospitality over the agreed amounts Financial Crime Team is responsible for reviewing and monitoring the Gifts and Hospitality register Group Legal Director is responsible for reviewing and signing off as required any ex-gratia payments or legal settlements as requested from the Business. Human Resources is responsible for any incidents where further action is required and ensuring completion of mandatory training	Ongoing Ongoing
Political Donations/Lobbying	Employees making or soliciting political donations on behalf of Post Office may result in criminal prosecution.	Preventative Control: Before giving or offering Hospitality to or from a political party, approval must be obtained from a GE Member. The giving of political donations or gifts on behalf of the group to a Politician or a Political Party is~~are~~ strictly prohibited.	Each employee is responsible for ensuring that all Gifts & Hospitality offered or received is recorded Group Executive are~~is~~ responsible for the approving or declining of any offers of hospitality by a political party	Ongoing Ongoing

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
		Post Office has a Group wide training programme to ensure that all customer facing staff, back office staff and contractors receive adequate training. Staff and contractors are required to complete training within 30 days of joining Post Office and annually.	Financial Crime Team is responsible for reviewing the Gifts and Hospitality register Human Resources is responsible for any incidents where further action is required and ensuring completion of mandatory training	Ongoing
Procurement/Third Party Risk	Inadequate monitoring may lead to third parties engaging in bribery or corruption while performing services on behalf of the Post Office Group. This could result in criminal prosecution, loss of key contracts or reputational damage.	Preventative Control: Post Office ensures that any fees paid are proportional to the services being rendered or consistent with the market. New and existing contracts are reviewed on an ongoing basis to ensure that there is no risk of conflicts of interest. This includes ensuring that all parties involved are aware of Procurement Lockdowns.	Chief Financial Officer Procurement	Ongoing Ongoing

The Group completes Annual Risk Assessments reviewing its bribery and corruption exposure and its compliance with the above key risk areas.

3. Definitions

3.1. Definitions

Bribery
Bribery is defined as the offer, promise, payment, request, agreement to receive anything of value whether directly or indirectly to or from any person or entity in order to induce that person or entity to perform their roles improperly or, in the case of a Public Official, in order to influence them with the intention of obtaining or retaining business or an advantage in the conduct of business.

Examples include an offer or promise to give anything of value to anyone to obtain or retain business for or on behalf of the Post Office or to obtain or fulfil a legal or regulatory requirement in furtherance of the Group's business. A bribe can take the form of a "reward" and be paid after the improper performance of the relevant duty or obligation.

Corruption
Corruption is defined as the misuse of entrusted power or public office for private gain.

Educational courses/conferences
Events that are offered by third parties without charge do not amount to hospitality. However, free places to attend courses or conferences that would otherwise attract a charge are covered by this procedure.

Facilitation Payment
A Facilitation Payment is a type of bribe and should be seen as such. A common example is where a government official is given money or goods to perform (or speed up the performance of) an existing duty. Within the UK these are strictly prohibited.

Gifts
Gifts refers to a physical gift and includes the offer to a specific individual or team with the exception of low value promotional items costing under £20 each, such as pens, calendars, diaries, notepads and paperweights.

Hospitality
Invitations to attend events which have a social element (whether or not they are at the same time as or linked to a business meeting) and where the cost of a 'ticket' (participation) is free of charge or reduced in price when otherwise there would be cost attached to it. This would include things such as tickets to a sporting event, tickets to a concert or a corporate dinner.

Inducement
An inducement is a benefit offered to a firm or any person acting on its behalf, with a view to that firm, or that person, adopting a particular course of action. This can include, but is not limited to, cash, cash equivalents, commission, goods, hospitality or training programmes.

Third Party funded trips
Travel/accommodation that is funded by third parties is covered by this procedure as a form of 'hospitality'.

4. Where to go for help

4.1. Additional Policies

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

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

4.2. How to raise a concern

Any Post Office employee who suspects that there is a breach in this Policy should report this without any undue delay.

In case of bribery or corruption concerns or whistleblowing, staff may contact:

- their line manager,
- a senior member of the HR Team, or
- if either or both are not available, staff can contact the Post Office's General Counsel, who can be contacted by email at: whistleblowing GRO or by telephone on: GRO
- Alternatively staff can use the Speak Up service available on GRO
- or via a secure on-line web portal: http://www.intouchfeedback.com/postoffice

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

4.3. Who to contact for more information

If you need further information about this Policy or wish to report an issue in relation to this Policy, please contact the Policy sponsor or Policy owner.

5. Governance

5.1. Governance Responsibilities

The Policy sponsor, responsible for overseeing this Policy is the General Counsel of Post Office Limited.

The Policy owner is the Director of ~~Risk and~~ Compliance who is responsible for ensuring that the Financial Crime Team conducts an annual review of this Policy and tests compliance across the Group. Additionally the Director of ~~Risk and~~ Compliance and the Financial Crime Team are responsible for providing appropriate and timely reporting to the Risk and Compliance Committee and the Audit and Risk Committee.

The Audit and Risk Committee are responsible for approving the Policy and overseeing compliance.

The Board is responsible for setting the Group's risk appetite.

6. Control

6.1. Policy Version

Date	Version	Updated by	Change Details
November 2016	1	Georgina Blair	Roll out of Final version
June 2017	1.2	Thomas Richmond	Updated in line with comments from stakeholders
July 2017	1.3	Sally Smith	POL R&CC approval
September 2017	2	Sally Smith	Final Version approved by ARC
June 2018	2.1	Sally Smith	Annual revisions

6.2. Policy Approval

Group Oversight Committee: Risk and Compliance Committee and Audit and Risk Committee

Committee	Date v 2.0 Approved
POL R&CC	20th July 2017
POMS R&CC	31st August 2017
POMS ARC	18th September 2017
POL ARC	25th September 2017

Policy Sponsor: Group Director of Legal, Risk & Governance

Policy Owner: Director of ~~Risk and~~ Compliance

Policy Author: Head of Financial Crime

Next review: ~~August 2018~~June 2019

Company Details

Post Office Limited and Post Office Management Services Limited are registered in England and Wales. Registered numbers 2154540 and 08459718 respectively. Registered Office: Finsbury Dials, 20 Finsbury Street, London EC2Y 9AQ.

Post Office Management Services Limited is authorised and regulated by the Financial Conduct Authority (FCA), FRN 630318. Its Information Commissioners Office registration number is ZA090585.

Post Office Limited is authorised and regulated by Her Majesty's Revenue and Customs (HMRC), REF 12137104. Its Information Commissioners Office registration number is Z4866081.

Whistleblowing Policy

Author: Sally Smith Sponsor: Jane MacLeod Meeting Date: 10th July 2018

Executive Summary

Context

This paper sets out the updates and revisions to the Whistleblowing Policy as part of the annual review process for the Risk and Compliance Committee to consider and approve.

Questions addressed in this paper

- What changes to the Policy do we propose and why?
- What are the implications of these changes?

Conclusion

1. The Whistleblowing Policy has been amended to clarify the minimum control standards, roles and responsibilities
2. There are some minor changes to the requirements and minimum standards of controls which will be communicated to relevant stakeholders

Input Sought

The R&CC is asked to approve the updated Whistleblowing Policy.

The Report

Why do we need to review this Policy?

1. The Policy was last reviewed and approved by the R&CC in September 2017. The terms of the Policy require it be reviewed annually.

What changes to the Policy do we propose and why?

What are the key features that we propose and why?

2. There have been no legislation changes in the past year and no significant amends made to the policy at this annual review.
3. Minor amends have been made in relation to:
   - Revised definition of serious incidents in section 1.3
   - Updated with new link for Speak Up web portal
   - Added communication and awareness to all staff as minimum control standards
   - Included reference to Whistleblowing Officer nominated deputies to minimum control standards

How did we develop these recommendations?

4. Policy queries and issues that have arisen over the previous 12 months have been reviewed to ensure that these concerns are addressed.

What are the implications of these changes?

What will we need to do and by when, to implement and embed these Policy changes?

5. No material changes are required to comply with this updated Policy.
6. Internal communications and training – once the Policy has been approved, there will be a One communication to advise all employees of the changes and provide a link to the updated document on the Post Office Intranet.

What will the impact be on our wider business?

7. Transparency of Post Office's adherence and commitment to the Employment Rights Act 1996 and the Public Interest Disclosure Act 1998
8. The Financial Crime Team monitor adherence to the minimum control standards set out in the Policy on an on-going basis through their review of the Gifts and Hospitality Tool and any other reported issues - any control gaps identified are reported to the R&CC as required. Appendix A provides an overview of the assurance checks developed by the Financial Crime team during 2017/18.

What would the impact be of delaying approval?

9. Risk that the group breaches the Employment Rights Act 1996 and the Public Interest Disclosure Act 1998 by not having up to date policies and procedures to provide protections to whistleblowers.
10. Post Office Limited is required to maintain up to date policies to support contractual requirements with clients and suppliers (e.g. MoneyGram and the Partner Banking Framework) and failure to do so may result in a breach of contract, and whilst not material, could have commercial and reputational impacts.

11. Post Office Limited provides Post Office Management Services (POMS) with its policies suite in the form of "Group Policies". POMS is required under its regulatory responsibility to the Financial Conduct Authority to have up to date policies and failure to do so may lead to regulatory sanctions or penalties.

Appendix A - Minimum Control Standards Assurance

The below table shows the residual risk rating from a first and second line of defence perspective for each control type within the currently approved policy as at the Q1 2018/19 review

Risk Description	Control Type	Description of control	Residual risk rating			Control Strength		Q1 Assurance Comments
			L	I	S	1st LoD	2nd LoD	
Failing to investigate the whistleblowing report and take necessary action	Directive	(a) Nomination of a Whistleblowing Officer; (b) Regular reports to R&CC/ ARC; (c) Escalation process to the Audit and Risk Committee	1	2	2	Effective	Effective	Whistleblowing log spreadsheet maintained and monitored by Whistleblowing Officer and Financial Crime Team to ensure all investigations complete. Summary reports provided to R&CC and ARC regularly.
Failing to investigate the whistleblowing report and take necessary action	Preventative	(a) WB Policy; (b) training; (c) Escalation of WB reports; (d) comms	1	2	2	Effective	Effective	Whistleblowing comms launched in May, posters at all customer support centres, supply chain and DMBs. Intranet/One Article and DMB branch focus.
Failure to ensure confidentiality for the whistleblower	Preventative	(a) WB policy; (b) Speak Up line reporting; (c) designated WB email inbox; (d) WB confidentiality arrangements	1	2	2	Effective	Effective	Access to systems restricted to Whistleblowing officer and nominated deputies. Documented process is currently being reviewed and re-drafted. Details regarding Whistleblowing found on 'My HR' page are being updated.
Failure to ensure confidentiality for the whistleblower	Corrective	(a) WB breach escalation process	1	2	2	Effective	Effective	Only Whistleblowing Office and nominated deputies have access to reports. Where these need to be referred to other parties to initiate investigations then a standard confidentiality statement and instructions are included in the request.
An individual may raise a whistleblowing report with other individuals in the Group. Details may then be shared with various stakeholders before being passed onto the Whistleblowing Officer	Preventative	(a) WB policy; (b) training; (c) comms.	1	2	2	Effective	Effective	Training provided to Grapevine, NBSC, Customer Support and ECT August 2017 and additional comms have been undertaken since. Plan to provide further training during Q2.

Risk Description	Control Type	Description of control	Residual risk rating			Control Strength		Q1 Assurance Comments
			L	I	S	1st LoD	2nd LoD	
An individual may raise a whistleblowing report with other individuals in the Group. Details may then be shared with various stakeholders before being passed onto the Whistleblowing Officer	Corrective	(a) WB breach escalation process	1	2	2	Effective	Effective	There have been no incidents where potential WB reports have not been sent to the Whistleblowing Officer, and further comms planned that will reinforce requirements
Failure to capture/report sufficient information about the issue may mean that the underlying issue cannot be properly investigated and resolved	Directive	(a) WB policy; (b) training.	2	2	4	Effective	Effective	Posters are on display at all back office sites and directly managed branches explaining to staff when and how to report. Additionally, Paula Vennals blog covered Whistleblowing and promoted the 'Speak Up' Line. My HR help page still directs employees to an out of date Whistleblowing policy' we are chasing to get this resolved. ABC Training due at end July and will incorporate whistleblowing awareness.
Failure to capture/report sufficient information about the issue may mean that the underlying issue cannot be properly investigated and resolved	Corrective	(a) Review of WB report database	2	2	4	Effective	Effective	There has only been one reporter where there was insufficient detail, this was reported by the Speak Up portal and they were requested to provide further information if they wished us to investigate. All reporters encouraged to give as much information as possible.
Failure to effectively record whistleblowing reports and pass onto the Whistleblowing Officer, due to factors such as resource or IT failure	Preventative	(a) Review of service and processes; (b) WB policy	1	2	2	Effective	Effective	Contract with InTouch Ltd has been reviewed (Now called Expolink Europe Ltd). There have been some enhancements to the services and reporting that they provide to their clients. No issues identified with provider. Internal processes will be reviewed over the next quarter.
Breach of whistleblowing guidelines such that a whistleblower suffers	Preventative	(a) WB policy; (b) training; (c) comms.	1	2	2	Effective	Effective	ABC training due end of July, will include WB.

Risk Description	Control Type	Description of control	Residual risk rating			Control Strength		Q1 Assurance Comments
			L	I	S	1st LoD	2nd LoD	
prejudice as a result of making a report								

GROUP POLICIES

Whistleblowing Policy

Version – V2.1

Chief Executive's Endorsement

The Post Office Group is committed to doing things correctly. Our Values and Behaviours represent the conduct we expect. This Policy supports these to help us ensure that colleagues know how to report concerns regarding wrongdoing or dangerous practices and that they can do so without fear of recrimination.

1. Overview

1.1. Introduction by the Policy Owner

The General Counsel has overall accountability to the Board of Directors for the implementation of controls ensuring Post Office meets it Whistleblowing obligations. Whistleblowing is an agenda item for the Audit and Risk Committee and the Post Office board is updated as required.

1.2. Purpose

This Policy has been established to set the minimum operating standards relating to the management of Whistleblowing throughout the Group[1]. It is one of a set of policies which provide a clear risk and governance framework and an effective system of internal control for the management of risk across the Group. Compliance with these policies supports the Group in meeting its business objectives and to balance the needs of shareholders, employees[2] and other stakeholders.

1.3. Core Principles

Whistleblowing is the reporting of suspected wrongdoing and/or dangerous practices within[SS1] Post Office. This would include serious accidents, bribery, fraud, any criminal activity, ~~-~~regulatory breaches, miscarriages of justice, health and safety risks, damage to the environment, financial impropriety~~ and/or~~, reputational damage and/or any breach of legal or professional obligations.

In order to encourage Whistleblowing and provide appropriate protections to whistleblowers, the governance arrangements described in this Policy are based upon the following core principles:

- To encourage the reporting of any concerns as soon as possible in the knowledge that all concerns will be taken seriously and investigated, and that confidentiality will be respected;
- To provide guidance as to how to raise those concerns;
- To provide whistleblowers reassurance that all concerns are raised without fear of reprisals, even if they turn out to be mistaken;
- Post Office is committed to and oversees the implementation of a Policy in line with the Group's risk appetite. The Policy and associated procedures (set out or referred to in this document) are proportionate to the risks and complexity of the Group;
- Post Office undertakes a training and awareness program to ensure employees are aware of the Whistleblowing policy and procedure.

1.4. Application

This Policy is applicable to all employees within the Group and outlines the protections provided for whistleblowers by law. In order to encourage reporting of wrongdoing, Post

[1] In this Policy "Post Office" and "Group" mean Post Office Limted and Post Office Management Services Limited.

[2] In this Policy "employee" means permanent staff, temporary including agency staff, contractors, consultants and anyone else working for or on behalf of Post Office.

Office will, where appropriate, extend equivalent protection to Postmasters, Agent Assistants, and members of the public.

1.5. Legislation

The Group seeks to comply with all relevant UK legal and regulatory requirements including (but not limited to) the following legislation as amended or supplemented from time to time:

- Employment Rights Act 1996
- Public Interest Disclosure Act 1998

1.6. What is Whistleblowing

"Whistleblowing" refers to the act of exposing potential or actual wrongdoing and/or dangerous practices by reporting it either internally within an organisation, or to an external party. A whistleblower is a person who raises a genuine concern in relation to any wrongdoing, this includes criminal activity, miscarriages of justice, dangers to health and safety and the deliberate attempt to conceal it.

Individuals[3] should raise a concern if they are aware of, or suspect, wrongdoing which affects others (e.g. customers, members of the public, colleagues or the Post Office). The following lists some examples (this is a non-exhaustive list) of situations where an individual may raise a concern:

- Financial Crime including Fraud, Money Laundering and financing of terrorism,
- Giving, offering or taking of bribes,
- Financial mismanagement,
- Misreporting,
- Practices that could put individuals or the environment at risk,
- Breach of Post Office internal policies and procedures (including the Code of Business Standards),
- Tax Evasion,
- Concerns about slavery or human trafficking[4], and
- Any conduct likely to damage Post Office's reputation

Grievances and matters such as bullying and harassment are addressed under Post Office's HR policies and concerns in relation to such matters should be raised in accordance with the procedures set out in the appropriate HR policy.

If an individual is uncertain about whether something is within the scope of this Policy they should seek advice from the Whistleblowing Officer, whose contact details are set out in this Policy.

1.7. Protecting the whistleblower

Post Office has a statutory obligation to protect whistleblowers and will support any individual who raises genuine concerns under this Policy, even if they turn out to be mistaken. Post Office are committed to respecting the confidentiality of all whistleblowers, ~~and~~ including those who wish to remain anonymous.

[3] In this Policy "individuals" means Postmasters, Agent Assistants, members of the public and employees (permanent staff, temporary including agency staff, contractors, consultants and anyone else working for or on behalf of Post Office). The statutory protections offered under the Public Interest Disclosure Act 1998 only apply to employees, however Post Office Limited will consider extending these protections to other individuals where they have acted in good faith in raising concerns

[4] More information in relation to Modern Slavery can be found here - http://corporate.postoffice.co.uk/slaverystatement

Post Office will make every effort to protect the whistleblowers identity, however, it may be necessary in the course of an investigation to share this information with a relevant stakeholder (e.g. an investigator). There is no requirement for a whistleblower to provide personal contact information. However, not providing this information may reduce Post Office's ability to undertake a thorough investigation into the concerns raised.

Post Office will take all reasonable steps to ensure that whistleblowers do not suffer any detrimental treatment as a result of raising a concern. Detrimental treatment includes disciplinary action, dismissal, threats or other unfavourable treatment connected with raising a concern. Serious action will be taken against any individual who threatens or retaliates against whistleblowers in any way.

If an individual believes that they have suffered any such treatment, they should inform the Whistleblowing Officer immediately. The Whistleblowing Officer should take steps to address any victimisation, which may include working with the HR team to put appropriate measures in place. If the matter is not addressed the whistleblower should raise it formally using Post Office's Grievance procedure.

In all cases the individual's concerns will be treated sensitively and in confidence.

1.8. Whistleblowing Officer and 'Speak Up'

Post Office has ~~a~~ appointed the General Counsel as the Whistleblowing Officer who can be contacted on whistleblowing GRO

The Whistleblowing Officer will review concerns raised and determine the best course of action, if any. They may ask for further information in order to make this decision.

It is recognised that sometimes raising a concern directly with the business may not be possible. In such instances individuals should contact the "Speak Up" line, a confidential reporting service which is run by an independent company Expolink Europe Ltd (formerly known as InTouch MCS Ltd).

Contact details for the Speak Up line are:

- GRO
- https://wrs.expolink.co.uk/postoffice ~~http://www.intouchfeedback.com/postoffice~~ which is a secure on-line web portal[SS2]:

All reports to the Speak Up line will be acknowledged within five working days and will be passed to the Whistleblowing Officer.

It is also possible that individuals may whistleblow via a complaint to a front line team, e.g. Customer complaints, NBSC and Grapevine. These may be verbal or written communications.

In all instances any whistleblowing reports, regardless of reporting method, will be passed onto the Whistleblowing Officer. The whistleblower may be kept informed of any action taken, however, this information may be limited if it is required to keep the confidence of other people.

1.9. External Disclosures

The aim of this Policy is to provide an internal mechanism for reporting, investigating and remedying any wrongdoing in the workplace. In most cases individuals should not find it necessary to alert anyone externally.

However, the law recognises that in some circumstances it may be appropriate for individuals to report their concerns to an external body such as a regulator. The independent Whistleblowing charity, Public Concern at Work have a list of prescribed regulators for reporting certain types of concerns. Their contact details are as follows:

Helpline: GRO
E-mail: whistle GRO
Website: www.pcaw.co.uk

Public Concern at Work operates free, confidential advice to people concerned about crime, danger or wrongdoing in the workplace. Post Office strongly encourages advice is sought out from Public Concern at Work before reporting any concern to an external party.

Post Office Money Services (POMS) is directly regulated by the Financial Conduct Authority (FCA), Post Office Limited is an appointed representative of Bank of Ireland (UK) Limited. As such individuals may decide to whistleblow directly to the FCA, and can do so by using one of the following channels.

Helpline: GRO
E-mail: whistle GRO
Website: www.fca.org.uk/site-info/contact/whistleblowing
Address: Intelligence Department (Ref IDA), Financial Conduct Authority, 25 the North Colonnade, London E14 5HS

2. Risk Appetite and Minimum Control Standards

2.1. Risk Appetite

Risk Appetite is the extent to which the Group will accept that a risk might happen in pursuit of day to day businesses transactions. It therefore defines the boundaries of activity and levels of exposure that the Group are willing and able to tolerate.

The Group takes its legal and regulatory responsibilities seriously and consequently has[5]:

- **Tolerant risk appetite** for Legal and Regulatory risk in those limited circumstances where there are significant conflicting imperatives between conformance and commercial practicality
- **Averse risk appetite** for litigation in relation to high profile cases/issues
- **Averse risk appetite** for ligation in relation to Financial Services matters
- **Averse risk appetite** for not complying with law and regulations or deviation from business' conduct standards for financial crime to occur within any part of the organisation
- **Averse Risk Appetite** in relation to unethical behaviour by our staff.

The Group acknowledges however that in certain scenarios even after extensive controls have been implemented an action may still sit outside the agreed Risk Appetite.

2.2. Policy Framework

Post Office has established a suite of policies and procedures, on a risk sensitive approach which are subject to an annual review. The policy suite is designed to comply with applicable legislation and regulation. The Whistleblowing Policy should be considered and read in conjunction with other policies where relevant. These may include the Financial Crime Policy, the Anti-Bribery & Corruption Policy, Health & Safety Policies and HR Policies where relevant.

2.3. Who Must Comply?

All third parties who do business with the Group, including consultants, suppliers and business and franchise partners, will be required to agree contractually to this policy or have their own equivalent policy.

Any investigations will be carried out in accordance with the Investigations Policy which is available on the Post Office Intranet

[5] The Risk appetite was agreed by the Groups Board January 2015

2.4. Minimum Control Standards

A minimum control standard is an activity which must be in place in order to manage the risks so they remain within the defined Risk Appetite statements. There must be mechanisms in place within each impacted business unit to demonstrate compliance. The minimum control standards can cover a range of control types, i.e. directive, detective, corrective and preventive which are required to ensure risks are managed to an acceptable level and within the defined Risk Appetite.

The table below sets out the relationships between identified risk and the required minimum control standards in consideration of the stated risk appetite. The subsequent pages define the terms used in greater detail:

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
Receipt and investigation of whistleblowing reports	Failure to meet legal and regulatory requirements	Directive Control: Post Office must nominate a Whistleblowing Officer to receive reports, ensure that all reports are fully investigated and that any appropriate corrective action is undertaken.	Post Office CEO and Board	Ongoing
		The whistleblowing officer must provide a whistleblowing report to the R&CC and ARC at least annually.	Whistleblowing Officer	Annually
		Any serious whistleblowing concerns must be promptly escalated to the Chairman of the Post Office Audit and Risk Committee.	Whistleblowing Officer	Ongoing
		Preventative Control: All employees are trained and the policy is available to them	Whistleblowing Officer	Training must be provided at least annually

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
		The Whistleblowing Officer must ensure that appropriate arrangements are in place to ensure that whistleblowing reports are addressed promptly including during absences	Whistleblowing Officer	Ongoing
		Communications and awareness provided to all employees and Policy document published on the Intranet[SS3].	Head of Financial Crime	Annually
Breach of confidentiality	Failure to ensure confidentiality for the whistleblower	Preventative Control: Whistleblowing Policy Confidential Speak Up line reports are shared only with the Whistleblowing Officer and nominated deputies[SS4] Whistleblowing email inbox with access restricted ~~access~~to the Whistleblowing Officer and nominated deputies Whistleblowing Officer must put arrangement in place to protect the confidentiality of the whistleblower during investigations Corrective Control: All incidents of breaches are escalated to the Whistleblowing Officer to review and take necessary actions.	Whistleblowing Officer Whistleblowing Officer Whistleblowing Officer Whistleblowing Officer Whistleblowing Officer	Ongoing Ongoing Ongoing Ongoing Ongoing

Risk Area	**Description of Risk**	**Minimum Control Standards**	**Who is responsible**	**When**
Incorrect handling of whistleblowing report	An individual may raise a whistleblowing report with other individuals in the Group. Details may then be shared with various stakeholders before being passed onto the Whistleblowing Officer	Preventative Control: Training provided to contact teams to identify potential whistleblowing reports and ensure these are correctly handled, e.g.: • Grapevine, • NBSC, • Customer Support, and • Executive Complaints. Communications and awareness provided to all employees and Policy document published on the Intranet. Corrective Control: All incidents of breaches are~~ be~~ escalated to the Whistleblowing Officer to investigate and take appropriate actions.	Whistleblowing Officer Head of Financial Crime Whistleblowing Officer	Annually Annually Ongoing
Insufficient Information	Failure to capture/report sufficient information about the issue may mean that the underlying issue cannot be properly investigated and resolved	Directive Control: Employees are encouraged to report issues and provide full information and their contact details, where they feel able to do so Corrective Control: All reports, including those where insufficient information has been provided and no further action was taken are recorded on the Whistleblowing	Whistleblowing Officer Whistleblowing Officer	Ongoing Ongoing

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
		database, which is reviewed for trends and issues.		
The 'Speak Up' Service	Failure to effectively record whistleblowing reports and pass onto the Whistleblowing Officer, due to factors such as resource or IT failure.	Preventative Control: The Whistleblowing Officer must review the effectiveness of the service provided by Expolink Europe Ltd (formerly known as InTouch MCS Ltd) ~~InTouch Ltd~~ at least annually The Whistleblowing Officer must review the effectiveness of the processes operated by each of Grapevine, NBSC, Customer Support, and The Executive Complaints Team at least annually to ensure that whistleblowing reports are identified and communicated promptly.	Whistleblowing Officer Whistleblowing Officer	Annually Annually
Treatment of Whistleblowers	Breach of whistleblowing guidelines such that a whistleblower suffers prejudice as a result of making a report	Preventative Control Training must be provided to all people managers as part of their induction process as a manager and on appointment to Post Office Annual training must be provided to all Post Office staff to remind them of the protections available to whistleblowers and the	Whistleblowing Officer and HR Training Manager Whistleblowing Officer and HR Training Manager	Ongoing Ongoing

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
		importance of identifying and reporting wrongdoing The Code of Business Standards must refer to the whistleblowing policy and must be provided to all new joiners as part of their induction programme.	Whistleblowing Officer and HR Training Manager	Ongoing

3. Definitions

3.1. Definitions

Grapevine
24/7 Security Support Centre provided by Kings Ltd. Grapevine provide security advice and record all security incidents across the business, this includes burglaries, robberies and the reporting of suspicious activity.

Telephone Number: GRO
E-mail: grapevine.admin GRO

NBSC
Network Business Support Centre (NBSC) is a helpline and the first port of call for Post Office branches if they have any operational query or require assistance.

Telephone Number: GRO
E-mail: nbscenquiries GRO

Customer Support Team
Complaints handling team based in Chesterfield. The team address complaints reported into Post Office via various channels, including post and telephone.

E-mail: customercare GRO

Executive Complaints Team
This team handles all complaints addressed directly to the Group Executives. The team liaise with various stakeholders within the business in order to resolve complaints.

E-mail: flagcaseadvisor GRO

4. Where to go for help

4.1. Additional Policies

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

https://poluk.sharepoint.com/sites/thehub/SitePages/Key%20policies.aspx?web=1 ~~https://poluk.sharepoint.com/sites/postoffice/Pages/policies.aspx~~

4.2. How to raise a concern

Any Post Office employee who suspects that there is a breach of~~in~~ this Policy should report this without any undue delay. Whistleblowing can be reported via the following channels:

- Their line manager,
- A senior member of the HR Team, or
- If either or both are not available, staff can contact the Post Office's Whistleblowing Officer, who can be contacted by email at: whistleblowing GRO or by telephone on: GRO
- Alternatively staff can use the Speak Up service available GRO or via the secure on-line web portal: https://wrs.expolink.co.uk/postoffice ~~http://www.intouchfeedback.com/postoffice~~

In some instances it may be appropriate for the individual to report in the form of a complaint to Grapevine, the Customer Support Team or the Executive Complaints Team.

4.3. Who to contact for more information

If you need further information about this Policy or wish to report an issue in relation to this Policy, please contact the Policy sponsor or Policy owner.

5. Governance

5.1. Governance Responsibilities

As at the date of approval of this Policy, the General Counsel is both the Policy Sponsor and Policy Owner, responsible for oversight of the Policy.

The Audit and Risk Committee are responsible for approving the Policy and overseeing compliance.

The Board is responsible for setting the Group's risk appetite.

6. Control

6.1. Policy Version

Date	Version	Updated by	Change Details
April 2016	1.4	Jane MacLeod	Sponsors review and sing-off
August 2017	1.5	Vitor Camara	Annual Review and update.
September 2017	1.6	Thomas Richmond	POL R&CC approval
September 2017	2	Thomas Richmond	Final version approved
June 2018	2.1	Vitor Camara	Annual review and update.

6.2. Policy Approval

Group Oversight Committee: Risk and Compliance Committee and Audit and Risk Committee

Committee	Date version 2.0 Approved
POL R&CC	13th September 2017
POMS R&CC	31st August 2017
POMS ARC	18th September 2017
POL ARC	25th September 2017

Policy Sponsor: Group Director of Legal, Risk & Governance

Policy Owner: Whistleblowing Officer

Policy Author: Head of Financial Crime

Next review: ~~August 2018~~July 2019

Company Details

Post Office Limited and Post Office Management Services Limited are registered in England and Wales. Registered numbers 2154540 and 08459718 respectively. Registered Office: Finsbury Dials, 20 Finsbury Street, London EC2Y 9AQ.

Post Office Management Services Limited is authorised and regulated by the Financial Conduct Authority (FCA), FRN 630318. Its Information Commissioners Office registration number is ZA090585.

Post Office Limited is authorised and regulated by Her Majesty's Revenue and Customs (HMRC), REF 12137104. Its Information Commissioners Office registration number is Z4866081.

Whistleblowing Annual Report 2017-18

Author: Sally Smith

Sponsor: Jane MacLeod

Meeting Date: 10th July 2018

Executive Summary

Context

This report provides an overview of the financial year 2017/18 as part of our obligations to protect whistleblowers and support individuals who raise genuine concerns under the Whistleblowing Policy. The report provides a summary of the activities undertaken to raise awareness and evidence that all reports are properly investigated.

Questions addressed in this paper

- What issues have been highlighted based on the review?
- What actions need to be undertaken to mitigate any issues identified?

Conclusion

1. The whistleblowing reports received have not identified any significant areas of concerns nor do they indicate any systemic problem within the Post Office. The majority have been from agents or agent assistants, which Post Office treats in the same way as employees under the Employment Rights Act 1996 and the Public Interest Disclosure Act 1998.

2. A complete review of whistleblowing reporting channels and processes has been undertaken to enhance controls and business communication and awareness has improved.

Input Sought

The RCC are asked to review the contents of this report and advise any further actions required.

The Report

Summary of activities relating to Whistleblowing reporting 2017-18

1. The whistleblowing policy was reviewed, updated and approved in September 2017.
2. During 2017-18, the Whistleblowing Officer appointed as nominated deputies, individuals within the Financial Crime Team to monitor and manage whistleblowing reports and investigations on a day to day basis.
3. A review of the whistleblowing process and report log was conducted by the Financial Crime team to ensure compliance with policy. As a result a number of historic cases were reviewed and closed, and training and guidance was given to NBSC, Grapevine, the Executive Complaints Team and Customer Support to help them identify any complaints that should be reported to the Whistleblowing Office and treated accordingly.
4. New processes have been implemented to ensure that those parties within Post Office who have to be involved in investigations into allegations are fully aware of their responsibilities and the confidential nature of their investigations.
5. Access rights were reviewed for the Whistleblowing Mailbox and the Speak Up Line portal to ensure access was appropriate.
6. The Speak Up service was promoted through both Paula's blog and the February 2018 Team Talk Plus.
7. The contract with ExpoLink Europe Ltd (formerly InTouch MCS Ltd), provider of the Speak Up service has been reviewed and was due for renewal in April 2018. This is being renewed, together with a contract variation to comply with recent GDPR changes.

Summary of Whistleblowing reports received 2017-18

8. During 2017-18, 37 whistleblowing reports were received and 33 cases were closed.
9. The majority of the allegations were about Postmasters or Agent Assistants (22 reports). There were 7 reports made about Post Office employees.

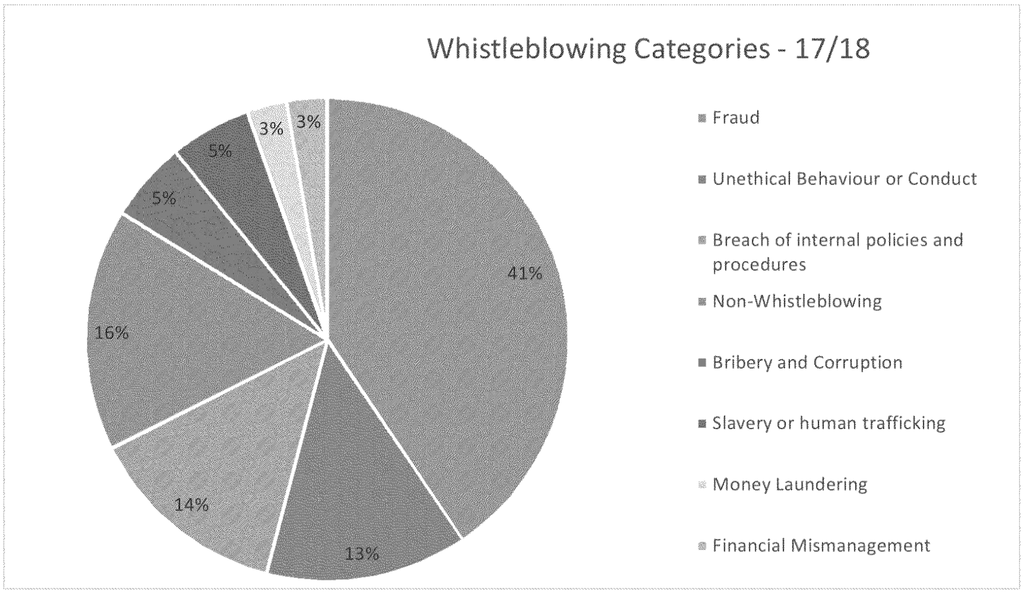
Allegations reported by 2017/18	Volume
Anonymous	10
Postmaster	9
Agent Assistant	6
Unknown	4
Direct Employee	3
Third Party*	3
Member of the public	2

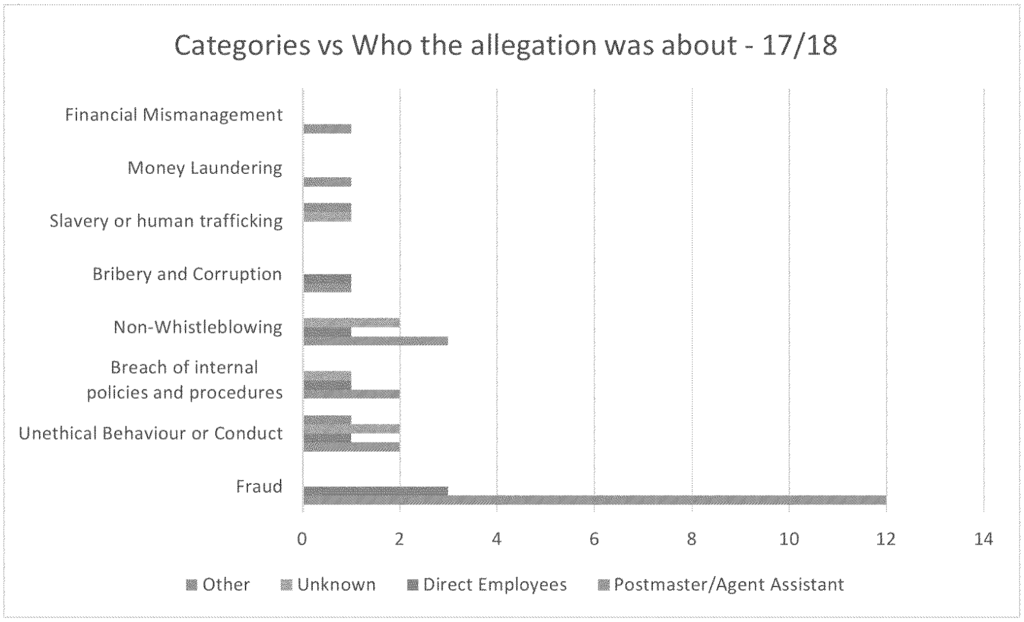
*This includes the Police, Royal Mail and Bank of Ireland

Who the allegation was about 2017/18	Volume
Postmaster	12
Agent Assistant	10
Direct Employee	7
Unknown	6
Post Office Ltd	1
Branch	1

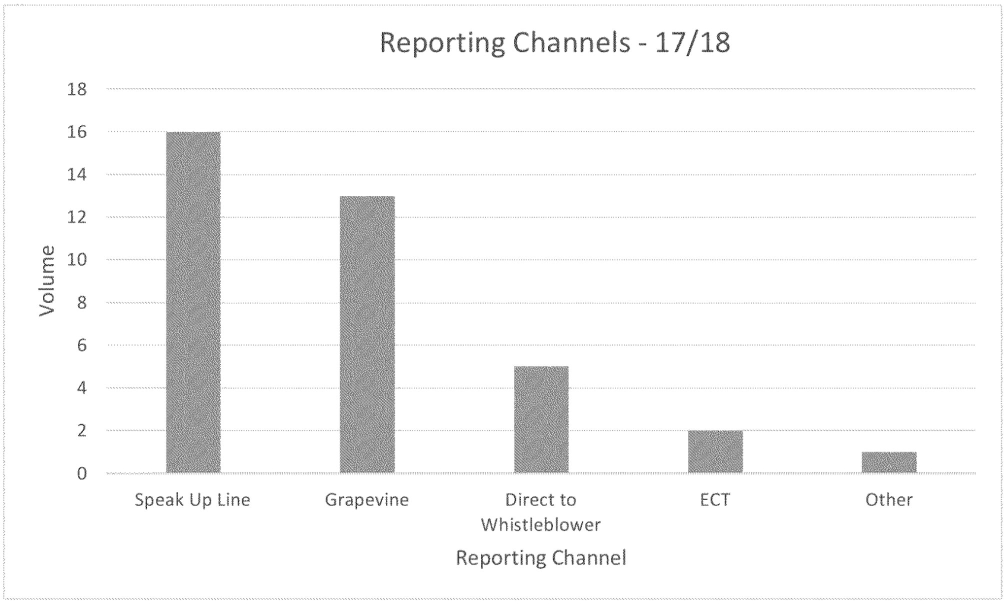
POL00401627

10.41% of the reports received were allegations of fraud. Predominately this was about either a Postmaster or Agent Assistant (12), however, there were 3 reports involving Post Office employees.





12.The most popular channels used to report concerns were the Speak Up line (16) and Grapevine (13).



13.The whistleblowing reports have not identified any route cause which may indicate a systemic problem. However, some investigations have led to further issues being identified at branches and appropriate corrective action has been taken. This includes temporary suspensions of Postmasters.

Activities planned for 2018-19:

1. A communications campaign went live at the start of 2018-19 and this has so far included a Branch Focus Article for DMBs, an Intranet Article, Yammer posts and whistleblowing awareness posters at all Customer Support Centres, Supply Chain sites and DMBs.
2. The following activity is planned:

- Continuous communications and awareness.
- Whistleblowing Policy annual review and update July 2018
- Expolink Europe Ltd (InTouch MCS Ltd) contract renewal to be finalised.
- Process documents across all areas to be reviewed and updated.
- The Financial Crime Team to review the functionality and performance of the Expolink Ltd case management system to ensure it meets Post Office requirements and contractual commitments.