UKGI00021233

Post Office Audit, Risk and Compliance Committee Agenda

Date
31 July 2018

Start Time	Finish Time
09.30hrs	11.00hrs

Location
Room 1.19 Wakefield

Present	In Attendance		Apologies
• Carla Stent * • Tim Franklin (Chair) • Tom Cooper • Ken McCall	• Paula Vennells • Al Cameron • Tim Parker • Johann Appel • Jonathan Hill • Jane MacLeod • Lisa Toye (Secretary)	• Micheal Passmore (4) • Rob Houghton (9) • Mick Mitchell (9)	• Jenny Ellwood
* Participation by conference call			

Agenda Item		Action Needed	Purpose	Lead	Time
1.	**Welcome and Conflicts of Interest**			Chairman	09.30
2.	**Minutes of the previous meetings, Matters Arising and Actions List**	Approval	To approve the minutes of the previous meetings, note the matters arising and update on the actions.	Chairman	09.30 – 09.35 (5 minutes)
3.	**Updates from Subsidiaries**				09.35 – 09.40 (5 minutes)
	3.1 POMS ARC Report	Questions & Noting	To receive a verbal update from the POMS ARC.	Tim Franklin	
4.	**Appointment of the External Auditor**				09.40 – 9.55 (15 minutes)
	4.1 Audit Tender and Appointment Report	Approval & Recommendation to the Board	To review the outcome of the audit tender and recommend appointment of the external auditor to the Board.	Micheal Passmore	

CONFIDENTIAL

UKGI00021233

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

Agenda Item	Action Needed	Purpose	Lead	Time
5. Internal Audit				9.55 – 10.05 (10 minutes)
5.1 Internal Audit Co-source Appointment	Noting	To ratify the decision made by correspondence.	Johann Appel	
5.2 Internal Audit Report	Questions and Noting	To note the Internal Audit Report. (The ARC Committee is reminded supplementary reading will be published in the reading room.)	Johann Appel	
6. Risk Update	Questions and Noting	To review the consolidated (including IT and Change) Risk report.	Jane Macleod	10.05 – 10.20 (15 minutes)
6.1 Risk Report				
7. Compliance Update	Questions and Noting	To review the consolidated Compliance report.	Jonathan Hill	10.20 – 10.30 (10 minutes)
7.1 Compliance Report				
7.2 Vulnerable Customers Risk Assessment and Gap Analysis	Questions and Noting	To review and comment on the proposed actions in the work plan.	Jonathan Hill	10.30 – 10.40 (10 minutes)
7.3 Whistleblowing Annual Report	Noting			Noting Only
7.4 Gifts and Hospitality Annual Review	Noting			Noting Only
8. Policies				10.40 – 10.45 (5 minutes)
8.1 Review of Anti-Bribery and Corruption Policy Report	Noting	To review the proposed policy updates.	Jane MacLeod	
8.2 Anti Bribery and Corruption Policy	Approval	To approve the policy (published in the reading room).	Jane MacLeod	
8.3 Review of Whistleblowing Policy Report	Noting	To review the proposed policy updates.	Jane MacLeod	
8.4 Whistleblowing Policy	Approval	To approve the policy (published in the reading room).	Jane MacLeod	

UKGI00021233

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

Agenda Item	Action Needed	Purpose	Lead	Time
9. Updates for Noting 9.1 Compliance with Payment Card Industry Data Security Standards	Questions & noting	To receive an update on compliance with PCI-DSS.	Rob Houghton / Mick Mitchell	10.45 – 10.55 (10 minutes)
10. Any Other Business		Topics raised under Any Other Business.	Chairman	10.55 – 11.00 (5 minutes)

UKGI00021233

Post Office Limited
ARC Committee Meeting

MINUTES OF A MEETING OF THE AUDIT, RISK AND COMPLIANCE COMMITTEE (THE "COMMITTEE") OF POST OFFICE LIMITED (THE "COMPANY") HELD ON TUESDAY, 27 MARCH 2018 AT 20 FINSBURY SREET, LONDON EC2Y 9AQ AT 09.00AM

Present:	Carla Stent	Committee Chairman	
	Richard Callard **(RC)**	Non-Executive Director	
	Tim Franklin **(TF)**	Independent Non-Executive Director	
	Ken McCall **(KM)**	Senior Independent Director	
			Item
In Attendance:	Tim Parker **(TP)**	Group Chairman	
	Tom Cooper **(TC)**	UKGI, Incoming Non-Executive Director	
	Paula Vennells **(PV)**	Group Chief Executive (CEO)	
	Alisdair Cameron **(AC)**	Chief Finance and Operations Officer (CFOO)	
	Jane MacLeod **(JM)**	Director, Legal Risk and Governance	
	Sarah Koniarski **(SK)**	Assistant Company Secretary	
	Ashish Singh **(AS)**	Head of Risk	
	Johann Appel **(JA)**	Senior Manager Internal Audit	
	Peter McIver **(PM)**	Ernst & Young	
	Claire Johnson **(CJ)**	Ernst & Young	
	Jonathan Hill **(JH)**	Head if FS&T Risk and Regulation	*(Item 6.1)*
	Steve Ashton **(SA)**	Chairman, Post Office Management Services Limited	*(Item 3.1 via conference call)*
	Rob Houghton **(RH)**	Group Chief Information Officer (CIO)	*(Items 4.5, 4.6, 9.3 and 9.4)*
	Sally Smith **(SS)**	Head of Financial Crime	*(Item 4.4)*
	Martin Kearsley **(MK)**	Banking Director	*(Item 5.1)*
	Richard Williams **(RW)**	Senior Risk Manager	*(Item 6.1)*
	Deana Herley **(DH)**	Senior Assurance Manager	*(Item 6.1)*
	David Gemmell **(DG)**	GDPR Programme Manager	*(Item 8.1)*
	Chris Russell **(CR)**	Senior Data Protection Officer	*(Item 8.1)*
	Nicholas Spicer **(NS)**	Payments Acceptance and Industry Relations Manager	*(Item 8.2)*
	Jules Harris **(JH)**	Head of Information Protection & Assurance	*(Item 8.2)*
Apologies:	Amanda Bowe	Chairman, Post Office Management Services Limited ARC Committee	

1. WELCOME AND CONFLICTS OF INTEREST

A quorum being present, the Chair opened the meeting. The Directors declared that they had no conflicts of interest in the matters to be considered at the meeting in accordance with the requirements of section 177 of the Companies Act 2006 and the Company's Articles of Association.

SA joined the meeting by telephone.

UKGI00021233

2. MINUTES, MATTERS ARISING AND ACTIONS LIST

The minutes of the meeting held on 29 January 2018 were approved and authorised for signature by the Chairman subject to an amendment to record a supplementary discussion under the Annual Legal Risk Report relating to State Aid and the relationship with the shareholder.

The actions 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. UPDATES FROM SUBSIDIARIES

3.1 POMS ARC Committee Report

The Chair welcomed SA to the meeting to provide an update on the work of the Post Office Management Services Limited ("POMS") Audit, Risk and Compliance Committee ("ARC"). The following had been considered at a meeting of the POMS ARC held on 14 March 2018:

(a) Risks outside of risk appetite

SA provided an overview of the top five risks which were considered to be outside of POMS risk appetite, particularly:

- the Appointed Representative ("AR") risk with Post Office as distributor of insurance products and services;
- the POMS Strategy, which had been recommended by the POMS Board to the Post Office Board for endorsement;
- premium reconciliation, although the POMS ARC had been satisfied this risk would move within appetite by May 2018;
- compliance with the General Data Protection Regulations ("GDPR") by the May 2018 deadline; and
- a shortage of central marketing infrastructure and capability, although actions to mitigate the risk were being implemented and the ARC expected this risk to diminish by May 2018.

(b) Referring in detail to the controls POMS should have in place to demonstrate both to internal management and to its regulator the effective oversight of the AR risk, SA conveyed that the ARC had examined the range of controls in operation and had considered how they could be strengthened to bring the risk within appetite. Although progress was broadly on track, the ARC had identified some pressure on prioritisation of systems and recognised that training would need to be developed to strengthen the competency of branch colleagues. The July POMS Board would review progress and the recommended controls.

(c) Roger Gale (RG) had attended the meeting on behalf of Debbie Smith (Chief Executive Retail) to provide an update on branch monitoring. Discussion had led to consideration of strategic forward planning and it was agreed that the insurance strategy should align with the Post Office Retail Network strategy. Both shared a common goal to promote optimal sales compliantly whist engaging branch colleagues.

(d) SA highlighted the process of implementing the changes required to achieve compliance with the General Data Protection Regulations ("GDPR") and their impact on POMS. The POMS ARC had considered the GDPR risk to be rated red but expected it would improve to amber shortly after the 25 May compliance deadline. Work was underway to reword literature for customer permissions online, in branch and in the call centre.

UKGI00021233

(e) Major Incident Reporting
SA explained that Hexaware hosted all data storage in the cloud and hosted POMS' main applications. A critical operational failure had lasted for 32 hours in February during which core systems were unavailable. The POMS ARC was reconsidering whether Hexaware remained an appropriate supplier and had discussed whether Accenture could support delivery of the services. Adverse weather has caused the Glasgow call centre to close and lessons were being learned. During the closure, customer behaviour had switched and increased online sales.

(f) Future Development
The POMS ARC had discussed the Insurance Distribution Directive and the implications of not being able to meet the regulatory deadline by the end of the calendar year. It was estimated that failure to do so would result in losses of approximately £0.8m per annum. The POMS ARC had also noted that the Financial Conduct Authority was increasingly focused on pricing, particularly renewals versus new policies. The POMS ARC was mindful of changes to the shape of customer propositions and recognised the need to future-proof the pricing strategy.

The Chairman thanked SA for his update.

SA left the meeting.

3.2 **Minutes of the POMS ARC Committee**

The Committee noted the minutes the POMS Audit, Risk and Compliance Committee meeting held on 13 December 2017.

4. MANAGEMENT OF KEY OPERATIONAL RISKS

4.1 **Financial Reporting Controls**

The Financial Reporting Controls Framework report was taken as read. TF commented that good progress had been made on developing the controls but observed that a significant proportion were either not sufficiently evidenced or were not operating effectively. TF asked how management of those controls could be embedded into performance management. AC responded that there was an expectation that reporting would be submitted on time and evidenced. This had been supported by the potential for disciplinary action should an individual repeatedly fail to meet expectations. Lessons were also being learnt following feedback from PwC and the recently concluded Internal Audit report, which would be submitted to the May ARC.

The Committee discussed the Joiners, Movers and Leavers remediation work. JM advised that work throughout the year, particularly relating to IT had flagged recurring issues and EY was confident that progress was being made to close the gaps, particularly through the implementation of improved procedures. Responding to the Chairman, JM confirmed that manual controls were now in place across all of the areas which had been identified as weak. IT were working on the next phase to scope an automated solution and a proposal was expected by the end of April. The manual controls did carry a significant dependency on line managers to initiate the process. Testing for inactive accounts assisted to identify oversights. KM asked whether the automated solution had been included in the IT roadmap. JM explained that initial work via the change process had been

UKGI00021233

delayed owing to the costs quoted by suppliers. A holistic solution was being developed by Post Office IT and the scope of the work would be confirmed by the end of April. Funding approval would then be sought via the change process and it was expected that implementation would span approximately 3 to 4 months.

The Financial Reporting Controls report was noted.

AC advised the Committee that a new format of reporting would be developed for the July ARC meeting which would combine assessment of the financial controls with the Placemat to create an enhanced style of reporting. The Committee recognised that the control framework had evolved since its inception and it was hoped that a new approach would assist to facilitate deep dives, focusing on particular areas of risk and compliance as needed.

4.2 **Financial Services Conduct Risk Update**
The Committee noted the Financial Services Conduct Risk Update.

4.3 **Change Risk Update**
The Committee noted the Change Risk Update.

SS and RH joined the meeting.

4.4 **Financial Crime Risk Update**
SS presented an update on financial crime risks including those relating to Anti-Money Laundering ("AML"), Counter Terrorist Financing ("CTF") and Anti-Bribery and Corruption. The paper was taken as read and SS drew the Committee's attention to the following in particular:

(a) Bureau de Change products to be delivered during 2018/19, included enhanced data monitoring capabilities, eKYC checks, politically exposed persons and sanctions checking for transactions over £0.2m. SS provided an update on Post Office's ongoing dialogue with the regulator. Recent meetings had demonstrated that policy officers within HMRC were not aligned on their requirements. HMRC had previously indicated that it would not require the Post Office to retain a copy of customers' identification for transactions above £0.2m. Recent correspondence had suggested that HMRC was considering reverting to a requirement to keep a physical copy of customers' identification. Complying with this requirement would carry a significant impact for the Post Office.

(b) A further dimension of the dialogue was the Fit and Proper regime and its impact, not only in respect of Postmasters and their employees, but also where there was corporate engagement the owners of those branches would be subject to the regulatory requirements. The Company would be required to demonstrate the fitness and propriety of all agent entities to HMRC, providing the requisite information by 25 June 2018. Compliance with the requirements would carry a significant operational impact, which would be resource-intensive. HMRC was aware that Post Office did not have all of the data requested (including information on directors and beneficial owners for limited companies which were corporate agents) and it was not stored on a single system. Any changes would need to be notified to HMRC within 30 days otherwise HMRC would de-register either the impacted branches or Post Office. Additionally, to date, HMRC did not have a platform capable of receiving the information requested.

UKGI00021233

The Committee discussed whether there would be consistent application and enforcement across the industry but agreed that irrespective, the Post Office was considered to be a prominent high street brand and as such, focus on the Company's compliance would be inevitable. It was understood that both card payments and transactions conducted via the Customer Hub would assist to alleviate the problem for cash transactions exceeding £0.2m. It was acknowledged, however, that not all customers would use the Hub. SS expressed disappointment having worked closely with HMRC over the last year and showing a willingness to comply. The June deadline coincided with the Summer campaign which had created an additional pressure. SS had made clear to HMRC that the Company was actively pursuing compliance but given the late changes to what was required and the disproportionate demand on resources, more time was needed to reach full compliance. SS was collaborating with colleagues to escalate the issue within Government, particularly to the Treasury. **RC and TC offered to assist and SS requested SS to provide a written briefing note which would inform their discussion with the Treasury.**

The Committee noted the financial crime risk update report.

SS left the meeting.

4.5 **IT Risk Update**

The Chairman welcomed RH to the meeting. The IT Risk Update was taken as read. RH highlighted the following matters:

(a) Good progress had been made to eradicate gaps in the network estate and securing devices on the firewall with 10,600 network replacements having been made. A further 60 were due to be completed imminently and the remaining 40 would be completed by the end of March 2018. Referring to the Security Operations Centre, RH confirmed the firewall security protocol had been implemented and the Company could be confident that it had zero critical defects.

(b) The POLSAP migration had been delayed and this had further delayed IT disaster recovery testing. Although the full Horizon data centre fail over could not be carried out, risks were being mitigated through testing of primary to secondary connections and component failures. An end to end test was necessary and accorded with the design standards. It was anticipated the fail over would be scheduled for spring 2019 if not sooner. The stability of the infrastructure would continue to be monitored.

Responding to the Chairman, AC explained that he was working with RH to re-plan the timeline to September. Meeting the original target date of June would have compromised other areas to a degree which would have been outside of risk appetite. AC provided an example whereby the original cash setup on the transtrack had proved more complicated than anticipated. Consequently the pilot test site (Belfast) had slipped from January to March. Although it was now working, going live in June would have assumed that everything which had worked on the pilot site would function elsewhere without testing and this would be unacceptable, especially given the reliance on the system to process cash transactions. AC and RH believed that the delay would ensure realisation of the design standards agreed

UKGI00021233

at the outset of the project. Responding to KM, RH confirmed that compliance with GDPR would not be adversely affected by the POLSAP delay. Referencing the provision of a robust finance system, AC and PI agreed that prior to signing of the statutory accounts, the Company would need to satisfy itself and EY that it could confirm the items to be moved off POLSAP and demonstrate that the items which would be left behind could be properly written off without gaps. AC hoped that this would be achievable in May/June without delay to the original signing timetable.

The Committee recognised the intensive work which had been carried out to achieve the network migration and asked RH to convey it's thanks to the teams involved.

The Committee noted the IT Risk update.

4.6 **Cyber Security and Information Assurance Update**

The Cyber Security and Information Assurance Update was noted.

MK joined the meeting.

5. INTERNAL AUDIT

5.1 **Internal Audit Report**

The Committee noted the Internal Audit ("IA") report.

JA reported that delivery of the 2017/18 audit plan was making good progress. Year to date, fourteen reports had been completed, one had been cancelled, four reports were being cleared, six items of fieldwork were nearing completion, and four were due to begin. As at 28 February 2018, there were 41 actions open, three of which were overdue with legitimate reasons. Year to date, 119 audit actions had been completed. JA drew the Committee's attention to two IA reviews which had been completed since the last meeting. JA introduced MK who had joined the meeting to answer questions on the IA Banking Counter Services Framework Review.

The Chairman expressed her concern regarding the IA findings, particularly as the Banking Framework was relatively new and was a key component of the Company's strategic vision. IRRELEVANT

IRRELEVANT

The Chairman understood that participating banks would soon begin their own audits on the service provided by the Post Office. The Committee was clear that there were a number of actions to be closed, with solutions being embedded and tested, to diminish exposure before external audits commenced. The Committee sought assurance that work was underway to urgently close these actions.

MK acknowledged the Committee's concerns and explained that the Banking Counter Services Framework ("the framework") was the one of the first major contracts to be reviewed through the IA process. Many of the findings related to the support structures behind the contract. MK had been encouraged by the

IRRELEVANT

UKGI00021233

IRRELEVANT

IRRELEVANT MK referenced the summary of findings and their ratings, explaining that there were a number of P3 (low priority) actions being worked through. All of the P2 (medium priority) actions were on track to being resolved.

Addressing concerns relating to governance and lessons learnt, MK explained that the proposals had been through all of the appropriate gating approvals with the managers in the business at the end of 2015. The contract terms and the discussion points raised with those managers at the time had triggered a IRRELEVANT IRRELEVANT before the framework was brought into action. MK further explained that during 2016, there had been a great deal of internal change and some of the corporate knowledge had been lost in transition. Consequently, having navigated one approval process, the framework was not retrospectively re-submitted to the One Best Way approval process which was implemented by the business in 2016. MK suggested that this should of happened before go live and if it had, some of the issues identified by IA could have been fixed.

MK observed that some of the language used in the IA findings was not fully reflective of reality, providing inconsistent practices across the branch network as an example. MK explained that inconsistent processes across the banks was an inherent characteristic of the product and while the banks transitioned to new internal systems and processes, the Post Office had to transact with them in different ways. The Chairman reasoned that this would compound the need to ensure robust processes were in place, which were also capable of dealing with exceptions. MK concurred and provided an example of the Santander deposit process where every deposit was treated the same, having been managed by chip and pin regardless of value. Although the chip and pin remained the same and the deposit could only go to a single located business account, different employees might have deposited on each occasion and provided different forms of identification. This had flagged that there were inconsistencies in how individuals were identified but the account receiving the money had always been nominated, known about and chip and pin controlled.

Responding to the financial reconciliation issue, MK challenged the finding, stating that the process for invoicing was well controlled and based on the information supplied by Credence which was audited. Discussion ensued as to the inclusion of management comments and the Committee agreed that this element of IA reports could be improved and expanded. It was understood that this IA report had been subject to a number of discussions, particularly between management (MK) and the auditors and the management comment could have been more reflective of this. The Committee advocated the inclusion of comments from management where the findings were challenged.

Given the different processes used by banks, KM asked whether a process could be initiated by the Post Office to agree a form of standardisation. MK explained that the framework had set out standards for simplified transactions. A number of banks, however, were still IRRELEVANT

UKGI00021233

IRRELEVANT

Responding to KM, JA confirmed that of the 13 actions listed in the summary of findings, eight had been resolved and a further three were on track towards closure. JA was encouraged by the progress made in relation to addressing the priority findings. In respect of the P3 rated actions, JA explained that the audit had been thorough and had highlighted anything which could potentially result in non-compliance. For this reason there were a large number of P3 actions and JA would continue to work with MK to resolve.

The Committee turned its attention to the next steps. It was understood that the framework provided for an independent third party audit of the Post Office service with costs to be shared by the bank and the Post Office. It was noted that the proposal for costs had to be agreed by the Post Office before the start date was set. An external audit was imminently expected in the next quarter and the Chairman reiterated the urgent need to close IA actions before the external audit commenced. The Committee thanked MK for his attendance.

TF referred to the delivery of the Change Assurance reviews which had been delayed because of difficulties in getting assistance from programme managers and executive sponsors. TF queried what could be done to address the problem and perform the reviews. JA explained it had been difficult for Deloitte to gain access to the change projects to deliver assurance. There was a new Head of Change Assurance who was working with IA to address the challenges. JA added that the move to agile delivery had complicated matters. TF suggested that the tender for

IRRELEVANT

IRRELEVANT JA reassured the Committee that this had been included in the RFD for the new provider. The Chairman added that lessons learnt from previous change projects would also need to be taken forward to address the internal challenges. PV and JA agreed to meet outside of the meeting to discuss how the adoption of change within the business and the understanding of agile methodology could be supported.

Responding to the IA findings on the Customer Complaints process, TC queried how the data on the volume of complaints was reported. The Chairman confirmed that the ARC saw the data based on each of the verticals rather than thematically. JM added that for POMS and the Bank of Ireland products, which were regulated, there was a detailed complaints reporting and analysis process. Complaints relating to other products and services had historically been subject to a less joined up process. The IA findings acknowledged that complaints arrived via several channels in significant volumes and in varying levels of seriousness. The Customer Support team was based in Chesterfield and their output was reviewed on a monthly basis. The Committee intended to move towards considering areas thematically and the Placemat would facilitate this.

MK left the meeting.

5.2 **Audit Plan 2018/19**

The Committee reviewed the Internal Audit Plan 2018-19. RC recalled the potential acquisitions which could be made in 2018-19 and suggested an opportunity to

UKGI00021233

review lessons learned from a business integration perspective be accommodated in the plan. AC advised that a post-implementation meeting would be convened to review lessons learned and the Committee agreed that this discussion would not require an audit.

KM suggested that the format of the baseline plan for internal control reviews and the review of significant change activities could be improved. KM wished to be clear on the target reviews which 'must be done'. Responding, JA confirmed that the top 16 reviews in table 1 were listed in priority order and agreed that the balance could be moved to a watch list. Table 2 showed the current change portfolio of projects expected to request approval for funding. These needed to be monitored as they would likely require assurance supported by the co-source partner. JA highlighted section 14 of the report, the three year rotation plan, which showed the core processes for review in 2018-19.

The Chairman suggested that the priority of Q1 reviews be focused upon with the remainder to be assessed on a rolling basis. It was suggested that the spread of reviews also be re-evaluated to avoid pressure in Q4. The Committee understood the plan to be indicative and that it would be reviewed on a quarterly basis. The Chairman asked JA to accommodate the Committee's feedback in the next quarterly report.

The Committee noted the proposed Internal Audit Plan for 2018-19 and was satisfied that individually and collectively the reviews represented an appropriate programme to support senior management in their activities and to provide assurance to the Committee over key risks to the Post Office. The Committee noted that the timing of reviews within the year was subject to change.

5.3 **Review of the Internal Audit Charter**

The Committee receive a report on the Internal Audit Charter ("the charter") which was taken as read. Responding to RC, JA confirmed that the charter underpinned the governance for IA, establishing its independence and providing a mandate relevant to the performance of engagements. JA suggested that an annual renewal of the charter could be extended and sought the Committee's input. Following discussion, the Committee agreed to review the charter on a bi-annual basis.

TF observed that the charter was also a reference point for measuring the effectiveness of IA and **JA agreed to circulate the self-assessment as evidence of compliance with the requirements of the charter.** **JA**

The Committee noted the self-assessment as evidence of compliance with the requirements of the Internal Audit Charter and approved the Internal Audit Charter for continued use through 2018-20.

DH, RW and JH joined the meeting.

6. RISK UPDATE

6.1 **Risk Placemat, including an Update on Risk Exceptions and the Rollout of the Placemat**

The Chairman welcomed DH, RW and JH to the meeting. The Committee received a report on the Risk Placemat which was taken as read. The Chairman observed

UKGI00021233

that a number of risks in both POMS and Financial Services and Telecoms (FST&T) were rated as amber and requested an overview.

In respect of FS&T JH provided the following summary points:

(a) A total of 155 risks had been identified, 8 of which had been categorised as top risks. Knowledge resource was a key dependency owing to the scale of the work and expertise required. The CE of FS&T was leading improvements to resource and JH had also recruited to his own team, improving in-house expertise on compliance with telecoms regulations.

(b) FS&T did not have a structural disaster recovery business continuity plan. Work was underway, both within the directorate (JH for example had recently met with Fujitsu to work through a programme) and across the Company under the guidance of the Business Continuity Manager.

(c) JH highlighted the issues within financial crime, particularly the HMRC audit requirements for Travel Money, which the Committee had discussed earlier in the meeting.

(d) Referring to information protection, PCI-DSS and GDPR, JH was concerned that Fujitsu had demonstrated a lack of understanding. Particular to GDPR, the Telecoms, FS&T Risk and GDPR teams were working with Fujitsu on a remediation plan. It was hoped that the governance process around Post Office's relationship with Fujitsu would also be strengthened as Fujitsu was a key supplier to the business. JH was seeking to implement controls and oversight within Post Office and this increased rigour had been welcomed by Fujitsu.

(e) Highlighting increased regulation and the corresponding increased risk of non-compliance, JH explained that POMS was preparing for compliance with the Senior Manager and Certification Regime (SMCR). The FCA had confirmed that it did not have the statutory power to apply SMCR to Appointed Representatives ("AR") but it would be extending each regulatory breach across the wider financial services industry. This was expected to come into effect in 2019 and JH would be monitoring the implications for regulated products and services supplied by the Bank of Ireland and POMS. The Post Office was supporting POMS to deliver compliance and to provide comfort that its AR obligations were being met. JA was mindful that Ofcom (the communications regulator) frequently echoed measures rolled out by the FCA. The FS&T Risk team had maintained regular engagement with Ofcom on a one to one basis to ensure that Post Office was being pro-active in anticipating and gaining insight to regulatory change. In an effort to contribute to proposed change, the business had participated in various industry forums which were also attended by smaller competitors.

(a) Referring to the strategic risk linked to the financial strategy, JH reflected on the implications for the Customer Hub. There were a series of programme and wider stakeholder engagement risks to be managed, mitigated and controls to be put in place. A corporate governance approach was being developed which would align with the wider business and a detailed plan would be produced for the Customer Hub. A series of workshops would also be held across the company to increase stakeholder awareness and encourage contribution.

The Committee thanked JH for his update. It was understood that the report provided an indicative summary of the risks identified by teams within the Retail

UKGI00021233

directorate. The CE of Retail was reviewing these and would attend the July meeting to present a top down view. DH advised that GE was reviewing all red risks, having had oversight across the portfolio and would carry out a consistency based exercise to streamline the outputs. The Chairman was pleased that initial findings showed that the heat map corroborated the Committee's perception of risk, citing contract management, change and information protection as example recurrent themes across the business. The Committee agreed that granular information would support understanding of the key performance indicators from an objective perspective. The Chairman suggested that external information, such as data on complaints, would assist to calibrate the internal business perception. Internal information (IA observations being an example) would also provide greater insight.

Responding to a question from TF, RW explained that 60 per cent of the risks identified were new. The remaining 40 per cent had been tested to ensure that they were still fit for purpose and aligned to their capabilities. RW reminded the Committee that when a risk was pinned to the Placemat, it was being aligned to strategy and would link to the North Star. RW added that the aggregation process was challenging. JM supplemented that development of the Placemat would be a rolling process. The initial exercise was to ensure that the risks had been correctly identified, articulated and linked to the right controls. Each time these were tested, which was on a quarterly basis, any movements could be assessed. Effective controls were one of the influencers which could diminish a risk. DH and RW were considering how these movements would be illustrated on the Placemat.

TF asked whether completion dates which were set by teams (from the bottom up) were validated or challenged. RW explained that this was done during the quarterly review, after risks and actions had been identified. It was only carried out in respect of the top risks and progress against the actions and controls was closely monitored. DH supplemented that there were a large number of bottom up risks and work was underway to formalise the process for validating completion dates.

TF observed that the terminology used to describe PCI-DSS as a contractual requirement of the Banking Framework was misleading (section 6 of the report) because PCI-DSS was a legal requirement which carried serious fines for non-compliance.

KM queried the wider changes within the ATM industry which would potentially lead to the Bank of Ireland invoking a renegotiation of the ATM agreement. JH advised he would work with MK to address issues in this space. KM was keen to understand the implications. AC explained that there were material strategic challenges around the ATMs. There was a pressure to change the interchange fees which would in turn change their economic profile. The business was aware that the availability of ATMs on the high street was predicted to reduce by up to 25 per cent and the Post Office would need to assess its strategic position. The Committee acknowledged this would be a complex topic. It was noted that the ATM strategy be brought back to the Board for review.

RW, DH and JH left the meeting.

UKGI00021233

7. EXTERNAL AUDIT

7.1 External Audit Update

PM and CJ recalled for the Committee the audit timeline plan presented at the meeting held in November. Work had progressed well and in accordance with the plan. CJ confirmed that walk-throughs and testing of the controls were underway. Pre year end substantive testing in areas such as capital investments and revenue had been supported by AC's finance team. CJ advised that she had recently met with MP and members of the IT directorate to review the walk-throughs and testing of IT controls. EY was interested to understand the timing of issues which had arisen, particularly those towards the year end which had occurred after remediation had taken place. Referring to supporting evidence for the management letter, AC's team had responded to provide any additional information requested.

PM provided an update on the audit work relating to the postmaster litigation and Horizon. PM explained that he had met with JM and AC to discuss the status of the court proceedings. PM was also due to meet with JM and Andrew Parsons (Womble Bond Dickinson) in late April to receive a further update and review the need for a disclosure note. PM explained that to date, the claimants' had not indicated the amount of damages being sought and a formal state of claim was awaited. If a statement of claim was received prior to the signing of the annual report and accounts for the year ended March 2018, the Company would be required to disclose the figure as a contingent liability. This disclosure would be accompanied by a narrative to be drafted by JM and Womble Bond Dickinson for agreement by the Company. PM clarified that the figure disclosed would not need to be provided for because the Company would be making clear its intention to defend the matter. The Committee understood that EY would also assess whether the statement of claim affected its audit opinion and would prepare an emphasis of matter referencing the contingent liability. At present, the amount of damages sought was unquantified and PM would monitor the situation. JM added that there was a possibility that no indication of damages would be given until the forthcoming court hearings had considered the construction of the contract and the operation of Horizon.

DG and CR joined the meeting.

8. UPDATES FOR NOTING

8.1 GDPR Programme Update

The Chairman welcomed CR and DG to the meeting to provide a progress update on the project to achieve compliance with the General Data Protection Regulations ("GDPR") which would come in effect on 25 May 2018. DG, who had recently joined the Company as a GDPR Programme Manager, presented the report.

DG summarised that good progress had been made towards compliance but some areas of concern remained where work would need to be expedited to mitigate the risk. DG highlighted significant progress in the areas of employee and agent contracts since an update was provided to the ARC in January 2018. The remediation of supplier contracts, however, remained a key risk. There was reduced confidence in the likelihood of appropriate GDPR clauses being agreed and embedded by the May deadline.

UKGI00021233

The Chairman queried whether the compliance timeframe would accommodate the proposed contractual review of liability and insurance provisions to coincide with the GDPR amendments. CR explained that the review pertained to material contracts. Following evaluation, where improved liability and indemnity clauses would be commercially beneficial to the Company, a view would be taken on the balance of risk and whether further delays caused by the initiation of contractual negotiations would be in the best interests of the Company given the urgent need to comply with GDPR. CR added that the analysis was intended to address instances where the Company had an unreasonable exposure. The GDPR programme was working with contract and vendor manages to assess each agreement on a case by case basis.

The Committee sought clarification of the marketing consent risk arising from non-compliance in a contract between the Bank of Ireland ("BOI") and the Post Office. JL explained that under the agreement, BOI was the data processor and correspondingly the Post Office was the data controller. The contractual review initiated by the GDPR programme had confirmed that the Post Office marketing consent language would need to make clear to customers that the Post Office would own their data. Historically BOI had operated on the assumption that it had the right to market to those customers. Reconciling differing interpretations had taken time. JL confirmed that wording had now been agreed. In addition, protocols had been implemented to facilitate the sharing of customer information between both entities in accordance with customer consents. Responding to a question from the Chairman, CR confirmed that the customer consents only permitted BOI to market products and services provided by the Post Office. The Chairman asked a supplementary question regarding a customer's right to be forgotten. JL responded to confirm that the protocols enabled management of notifications between the entities and ensuring that information was reciprocated.

Discussion ensued regarding the possibility of customer consents not being received before the deadline. CR clarified that GDPR compliant wording would be used to seek consents from new customers. A risk analysis had been conducted to ascertain the cost and benefit implications of relying on legitimate interests to justify marketing to the back book. On balance it was considered to be more effective than conducting a paper exercise. The rationale for using legitimate interest was being documented on an individual basis for each product and service area.

The Committee noted the GDPR programme update and the material risks to effective compliance which would be monitored by the programme steering committee.

DG and CR left the meeting. JH and NS joined the meeting.

8.2 Compliance with Payment Card Industry Data Security Standards

The Chairman welcomed JH and NS to the meeting to present 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

UKGI00021233

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. The Committee expressed its concern that progress in achieving compliance had deteriorated and queried whether there had been a delay in bringing the escalating risk to its attention.

JH explained that the new standards (version V3.2) were more onerous requiring increased controls which, owing to the age of the Company's estate, were extremely challenging to implement. This was compounded by further areas of non-conformity which had been identified by the recently appointed external auditor. 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. CC was also disputing that its contract with Post Office required it to be PCI-DSS compliant and this had further delayed remedial action. The PCI Steering Committee was exploring different ways to achieve the necessary controls and as a precaution, change requests had been submitted to use Verizon and Fujitsu to address the gaps. Referring to the challenges JH explained that the depth of complexity had only transpired in the weeks leading to the March ARC meeting.

The Committee queried how the relationship with CC was being managed. JH explained that CC services had been procured in accordance with public procurement rules meaning that the services provided could not be extracted and directly awarded to a different provider. The PCI Steering Committee was exploring whether step-in rights could be used to fulfil the obligations. The Chairman enquired how negotiations to achieve the necessary controls could be supported. PV responded to confirm that she would support the CIO to escalate the matter to senior management within CC if needed.

The Chairman was concerned that failure to achieve the verified attestation on compliance by 31 July 2018 would also adversely impact the Banking Framework and reiterated the urgent need to resolve the situation within the timeline. It was understood that finding an alternative service provider was not an option.

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

JH and NS left the meeting.

9. POLICIES FOR APPROVAL

9.1 Treasury Risk Management Framework, Policies and Authorities

The Committee received a paper on the Treasury Risk Management Framework Policies and Authorities which was taken as read. The Treasury Policy had been updated following an annual review of the control framework and the proposed changes were detailed in sections 2 – 11 in the report.

The Committee discussed management of short-term liquidity, with particular reference to the Borrowing Policy (4.9) and therein access to a £950m working capital facility (the "BEIS Facility") provided by the Department of Business, Energy and Industrial Strategy ("BEIS") until March 2021. The policy explained the process to request a drawdown and how forecasting variances could lead to a shortfall between the amount drawn down and the actual amount required. TC referred to

UKGI00021233

the Facility Headroom (4.8.1) available under the BEIS Facility and noted that the Group aimed to maintain Facility Headroom of at least IRRELEVANT with any reduction in the Facility Headroom Buffer requiring Board approval. The Security Headroom was also being monitored and reported on a monthly basis. TC suggested that a headroom of equal importance was the amount Post Office borrowed from BEIS against its forecast. TC recommended inclusion of this headroom in the policy, particularly as it would be relevant to any business case for an overdraft submitted to the Treasury Committee.

TC asked a supplementary question regarding permitted levels of exposure for FX hedges, particularly how long FX could be hedged for. AC explained that borrowing would ordinarily not be longer than one month in duration. TC suggested that the policy should clarify that hedging either would not exceed one month in duration, or alternatively, would not exceed a certain level of exposure without escalation. The Committee supported TC's suggestions and AC undertook to oversee inclusion of these amendments in the policy.

The Chairman referred to the investment reserve balance of IRRELEVANT which could be varied during critical periods. The updated delegated authorities would authorise the Head of Treasury, Tax and Insurance to approve a temporary change to the investment reserve so that the target reserve balance would be in the range of nil to IRRELEVANT and for a maximum of IRRELEVANT Any changes outside of this range or for a longer period would require approval by the Chief Finance and Operations Officer (AC). The Chairman observed that the range permitted during critical periods was large and queried how frequently the increased range would be utilised. AC explained that it would be relatively infrequent and would likely be triggered when the IRRELEVANT overnight NRF facility (the amount available to be used under the NRF over the course of the Bank of England's financial year was constrained by a cap) had reached capacity. AC added that the two week maximum duration prevented the increase from being a routine occurrence. The Chairman was content to monitor any temporary changes to the reserve on the understanding that this provision may be brought back to a future ARC meeting for review.

The Committee approved the Treasury Risk Management Framework, Policies and Authorities (March 2018) subject to an amendment to the Headroom supporting policy guidelines (under section 4, Medium and Long-term Funding Management) and the inclusion of an exposure limit on derivative activity (FX swaps) under Corporate Treasury Activity (section 5, Counterparty Credit Risk Management). The CFOO was authorised to finalise these amendments.

9.2 **Document Retention and Disposal Policy**

The Committee received a report on the Document Retention and Disposal Policy which was taken as read. The policy set out a framework for compliance with a number of legal and regulatory requirements pertaining to the retention and disposal of different types of data. The report included a proposed implementation plan which, if agreed, would be undertaken through a separate work stream within the GDPR programme.

The Committee approved the Document Retention and Disposal Policy and agreed the implementation plan.

UKGI00021233

9.3 **IT Security Policy**

The Committee received a report and the draft IT Security Policy which was taken as read. TF referenced section 9 of the report which stated that IT Security would work with suppliers over the next year to understand and remediate gaps. TF asked whether the time frame was appropriate, particularly if there was any exposure to unmitigated risk. **RH undertook to reassess the timeframe and resubmit the report and policy to a future meeting.** **RH**

The Committee requested the policy be brought back for consideration to the May meeting.

9.4 **IT Disaster Recovery Policy**

The Committee received a report and the draft IT Disaster Recovery Policy which was taken as read. Responding to TF, RH affirmed that the policy requirements would be incorporated within third party contracts.

The Committee approved the IT Disaster Recovery Policy.

9.5 **Business Continuity Policy**

The Committee received a briefing note on the Business Continuity Management Policy which was taken as read. The policy had been updated following an annual review and the briefing note provided a high level overview of the status of work being managed against the policy.

The Business Continuity Management Policy was approved.

10. BUSINESS CONTINUITY

10.1 **Business Continuity and Crisis Management Update**

The Business Continuity and Crisis Management Update was noted.

11. GOVERNANCE

11.1 **ARC Effectiveness Review**

The Committee noted a report which evaluated the Committee's performance against its terms of reference in the previous year. The analysis concluded that the Committee had met the requirements with the exception of the requirement to review and update its terms of reference annually.

12. ANY OTHER BUSINESS

The Committee asked the Secretariat to provide feedback to contributors on reports, particularly regarding the length of reports and the detail in Executive Summaries.

There being no further business the Chairman declared the meeting closed at 11:04am.

....

Chair **Date**

UKGI00021233

Strictly Confidential

Post Office Limited ARC Committee

Status Report as at: 01 July 2018

Action included on the ARC agenda
Action recommended for closure
Action closed or not yet due

REFERENCE	ACTION	ACTION OWNER (GE MEMBER)	DUE DATE	STATUS	OPEN / CLOSED
22 January 2016 POLARC 16/03 (q)	Risk Update For the Executive to work with the external auditors to set out what a three year roadmap to benchmark against the UK Corporate Governance Code would like.	**Jane MacLeod (General Counsel)**	**October 2018 ARC**	The Chairman of the ARC & GC have agreed to revisit the benchmarking with the UK Corporate Governance Code in May 2018 (to coincide with the preparation of the 2017/18 Annual Report and Accounts). **May update**: benchmarking complete, will bring back to future meeting.	Open
25 September 2017 POLARC 17/75 (e)	Vulnerable Customer In discussion the Committee requested management to consider whether there are other organisations such as Citizens Advice, the Money Advice Service, Age Concern etc. that provide any form of 'kite marking' which we could use to benchmark the policy.	**Jonathan Hill**	**July 2018 ARC**	On July agenda.	To close
25 September 2017 POLARC 17/75 (g)	Vulnerable Customer Policy The Committee requested that the outcome of the risk assessment should be reported back to the Committee together with the resulting action plan.	**Jonathan Hill**	**July 2018 ARC**	On July agenda.	To close
23 November 2017 4.3 (d)	Change The Committee also requested that a 'lessons learned' be undertaken regarding SuccessFactors and for the project sponsor to report these back to the Committee.	**~~Martin Kirke~~ Mo Kang**	**~~July 2018 ARC~~ October ARC**	Deloitte were commissioned by Internal Audit to complete an independent lessons learned review of the SuccessFactors programme. This commenced mid-February with the aim of completing mid-March. The output from Deloitte has been delayed and the final report is due to be produced by the end of March. The SuccessFactors implementation has been very successful with only minor problems, automation of processes, reduced errors and 100% system availability.	Open
23 November 2017 & 29 January 2018 5.2 & 5.3 (Nov 17) 4.8 (Jan 18)	Information Security and IT Security Policies Review • Acceptable Use Policy Cyber and • Information Security Policy. (i) The Chair asked at what point would we be able to form a view that the cultural aspects had been embedded and were working, and whether this could be reviewed by Internal Audit? JA noted that IA are validating actions but should be able to provide a view following implementation of the final actions which are targeted for June. (ii) An update on IPA to be presented to the 2018 meeting.	**Jules Harris**	**October 2018 ARC**	(i) IPA are sending out a questionnaire 19/01/18 to give a baseline understanding of how well all staff understand their information security obligations before IPA start the new awareness campaign. This will be repeated in June, where an improvement is expected. Internal Audit have already got plans to review cyber security during 18/19 and have added a review of the effectiveness to the scope of that audit.	Open
17 May 2018 3.1	Update from POMS ARC Deep dive on POL responsibilities and performance as an Appointed Representative to be scheduled as a separate session within a future POL ARC meeting.	**Jane MacLeod (General Counsel)**	**October 2018 ARC**		Open
17 May 2018 4.1	ARA Cover Note - Migration from POLSAP to CFS The ARC sought assurance that the take on balance in CFS in September would be validated as accuracy from the outset would be imperative to its successful operation.	**Al Cameron**	**October 2018 ARC**	Referring to the mapping of accounts and transactions transferred from POLSAP and received in CFS, AC reported to June extraordinary ARC that a further review had provided additional comfort. Covering the previous three years of trading, the values amounted to a gross difference of £18k.	To close
17 May 2018 8.1	Compliance with PCI DSS Post Office was still without a Report on Compliance (RoC) from external qualified security assessors. It was Global Payments (GP) expectation that Post Office would receive a positive RoC by 31 July 2018. GP could levy a penalty against Post Office because of non-compliance. There were 112 open issues (across Computacenter and Fujitsu) of which 4 were identified as being at risk of not being remediated by 31 July. Post Office needed to host card data securely with the goal of protecting customers' data. Non-compliance caused significant risks to costs, revenue, reputation, the banking framework and relationships with clients and partners. This was an unacceptable position. The ARC requested the project manager to provide a timeline mapping deliverables. At its July meeting the ARC would review the plan, timelines for completion and accountability for each deliverable. In relation to the longer term strategic approach, the ARC requested an update on when the business case compiled by the Payment Services team would be ready for review. It was expected that an interim update could be provided by Rob Houghton at the Board Away Day in June.	**Rob Houghton / David Meldrum / Jules Harris / Nicholas Spicer**	**July 2018 ARC**	Report on the July agenda. PCI DSS Update: • 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	Open
17 May 2018 9.1	IT Security Policy The ARC supported the proposed changes to the IT Security Policy but observed that 16 standards (which supported the policy) were under review. JM advised that these were in development at a lower level overseen by the Head of IT Security. DM agreed to circulate an update on which standards had been reviewed.	**David Meldrum**	**July 2018 ARC**	The reviews have been completed. David Meldrum will circulate an update to the Committee, after its July meeting, to confirm.	Open
28 June 2018 2.4	Financial Results 2017-18 MP to confirm EY's receipt of the outcome of the 2014/17 POLSAP to CFS transfer proofing exercise. MP to work through the completeness of depreciation of fixed assets with EY.	**Micheal Passmore**	**July 2018 ARC (Extraordinary)**	Verbal update to be provided at July extraordinary meeting.	To close

UKGI00021233

External Audit Tender Update

Author: Micheal Passmore Sponsor: Al Cameron Date: 31 July 2018

Executive Summary

Context

The purpose of this paper is to update the ARC on the external audit tender process only, recommending the preferred choice and seeking ARC approval of the recommendation.

Questions addressed in this report

1. Who tendered for the bid?
2. What happened during the process and how did we ensure we complied with relevant requirements?
3. What happened at the presentation stage?
4. What were the final results of the scoring process and what is our recommendation?
5. What is the proposed cost quoted by the recommended auditor and how does that compare to other bidders and the current auditor?
6. Were there any other items to consider?
7. What are the next steps?

Conclusions

The Procurement was carried out using the Crown Commercial Service's Management Consultancy framework. The requirements under this framework and the best practice guidelines recommended by the FRC were followed where applicable to ensure a fair and consistent process.

Only two bids were received; both were scored on written proposals and again at the presentation stage. Scoring was performed using pre-defined scoring criteria.

Taking into account the moderated scoring and the Post Office panel views, IRRELEVANT

IRRELEVANT

Additional considerations were made around independence, and it was agreed that an

IRRELEVANT

UKGI00021233

Input Sought

We would like the ARC to approve the recommendation to appoint IRRELEVANT as provider of the Post Office Limited group external audit services.

The Report

1. Who tendered for the bid?

1.1 The Procurement was run using the Crown Commercial Services Management Consultancy Framework. Under this framework, the RFP (Request for Proposal) was issued to thirteen firms including 'big 4' and non-'big 4' firms.

1.2 We received two applications for the external services; one from IRRELEVANT and one from IRRELEVANT

2. What happened during the process and how did we ensure we complied with relevant requirements?

2.1 The written bids were reviewed and scored for both price and quality by Finance and Procurement. The scoring was performed independently by Micheal Passmore (Finance Director, POL), Danielle Goddard (Head of Financial Accounting & Governance) and Antony Ray (Senior Procurement Manager). All scoring was then discussed and moderated to provide an unbiased view.

2.2 The results of the scoring at this stage were: IRRELEVANT scoring highest at 83 points, followed by IRRELEVANT with 74 points.

2.3 The 9 additional points attributed to IRRELEVANT were predominantly in relation to: resourcing (2) as the proposal was for a Northern based team who have worked together on other engagements, with commitment to retaining the same team; IT audit capability (2) due to the bespoke approach described in the bid, the team's experience in back office IT transformation, and the innovative data auditing techniques described; audit approach (2) due to the efficient and tailored approach proposed to managing the audit; and fees (3) due to IRRELEVANT offering a more competitive fee.

2.4 Both firms scored fairly evenly in the other areas that they were marked on, including background and relevant experience; in-house technical resource; quality assurance and independence; information security, and business continuity.

2.5 As there were only 2 bids, both firms were taken through to the presentation stage.

UKGI00021233

2.6 In order to ensure we complied with the FRC best practice guidelines on audit tenders, we ensured that: the RFP was issued to a number of firms including non-'big 4' firms; the RFP included sufficient details about the business and bidders were allowed to ask additional clarification questions which were responded to promptly; scoring criteria was pre-defined, non-discriminatory, and consistent; and rationale was documented at each stage of the scoring process.

3. What happened at the presentation stage?

2.1 The Post Office scoring panel consisted of;
2.1.1 Carla Stent (Chair of the ARC committee)
2.1.2 Alisdair Cameron (CFOO)
2.1.3 Micheal Passmore (FD, POL)
2.1.4 Danielle Goddard (Head of Financial Accounting & Governance)
2.1.5 Antony Ray (Senior Procurement Manager)

2.2 Both IRRELEVANT were invited to present to the panel. They were assessed on their presentations, and on their answers to a number of additional questions from the panel.

2.3 After the presentations the bids were re-scored taking into account the views of the panel. These scores were then moderated again to give the final results. The final scores remained unchanged from stage 1.

4. What were the final results of the scoring process and what is our recommendation?

4.1 At stage 1 of the scoring process, the results were 83 points for IRRELEVANT and 74 points for IRRELEVANT After the scoring moderation following the presentations, these overall scores remained unchanged.

4.2 As IRRELEVANT scored the highest on points, it is on this basis that they are recommended as the preferred supplier.

5. What is the proposed cost quoted by the recommended auditor and how does that compare to other bidders and the current auditor?

5.1 IRRELEVANT were most competitive with an estimated annual cost of IRRELEVANT IRRELEVANT This figure may be subject to fluctuation depending on such factors as the changing size and complexity of POL at the time of each audit.

UKGI00021233

Thereafter the discounted pricing IRRELEVANT gave reduces by RPI on an annual basis. IRRELEVANT quoted fees of IRRELEVANT

3.1 EY audit and assurance fees (excluding over-runs) for the 2017/18 audit are IRRELEVANT. The IRRELEVANT quoted fees are IRRELEVANT lower than this, a reduction of 35%.

6. Were there any other items to consider?

6.1 **IRRELEVANT**

6.2 The POL presentation panel sought guidance from Tom Cooper (UKGI) as to whether UKGI felt this caused any potential conflict of interest.

6.3 **IRRELEVANT**

IRRELEVANT it would be helpful to have a second partner involved.

6.4 Subsequently, IRRELEVANT have assigned an additional partner to support IRRELEVANT in the provision of audit services, ensuring that he dually attends the ARC committee meetings. The additional partner also has public sector audit experience.

7. What are the next steps?

7.1 We require ARC to approve the recommendation to appoint IRRELEVANT as the external auditor.

7.2 We would then proceed to conclude some final commercial and contractual discussions with IRRELEVANT

7.3 The Board will then make the formal appointment.

UKGI00021233

POST OFFICE LIMITED NOTING PAPER

ARUDIT, RISK & COMPLIANCE COMMITTEE

Internal Audit Co-source Appointment

Author: Johann Appel Sponsor: Jane Macleod Meeting date: 31st July 2018

Executive Summary

Context

1. Internal Audit services are currently provided by IRRELEVANT (internal control reviews) and IRRELEVANT (change assurance reviews), with both firms operating under contract extensions since mid-2017.
2. A procurement exercise to replace these services with a single co-source provider was run under the Crown Commercial Services Management Consultancy Framework (RM3745, Lot 3 - Audit). The tender process was agreed with ARC during an extraordinary meeting held on 27 March 2018.

Process

3. Written bids were received from eight firms, which were scored for both price and quality. The three highest scoring eligible bids were then taken through to the presentation stage. IRRELEVANT was initially also invited, however, in line with the RFP rules they were excluded following the decision on the External Auditor appointment.
4. Following the presentations the bids were re-scored taking into account the views of all the presentation attendees. The final scores were as follows:

Bidder	Sore %
IRRELEVANT	

Financial Impact

5. Day rate and indicative annual cost, compared to current rates:

Blended day rate	IRRELEVANT
Indicative year 1 cost based on 490 days co-source support	

6. The IRRELEVANT blended day rate (using a weighting applied to the different levels of seniority from Consultant to Partner) is IRRELEVANT This was the third least expensive blended day rate of all the eight bids received. The indicative cost in year one of

UKGI00021233

the contract would be IRRELEVANT based on the approved 2018-19 audit plan, which requires 490 days of co-course support. The day rates offered by IRRELEVANT represent a cost reduction against the existing co-source agreements.

Recommendation

7. We recommended awarding IRRELEVANT with the option to extend this by a maximum of a IRRELEVANT. This recommendation was approved by all members of the ARC via e-mail on 18 July 2018.

Input Sought

The Committee is asked to note and formally ratify the appointment of IRRELEVANT as Internal Audit co-source provider.

UKGI00021233

Internal Audit Report

Author: Johann Appel Sponsor: Jane MacLeod Meeting date: 31 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 Audit, Risk and Compliance Committee (ARC) meeting in May and progress on delivery of the Internal Audit Plan.

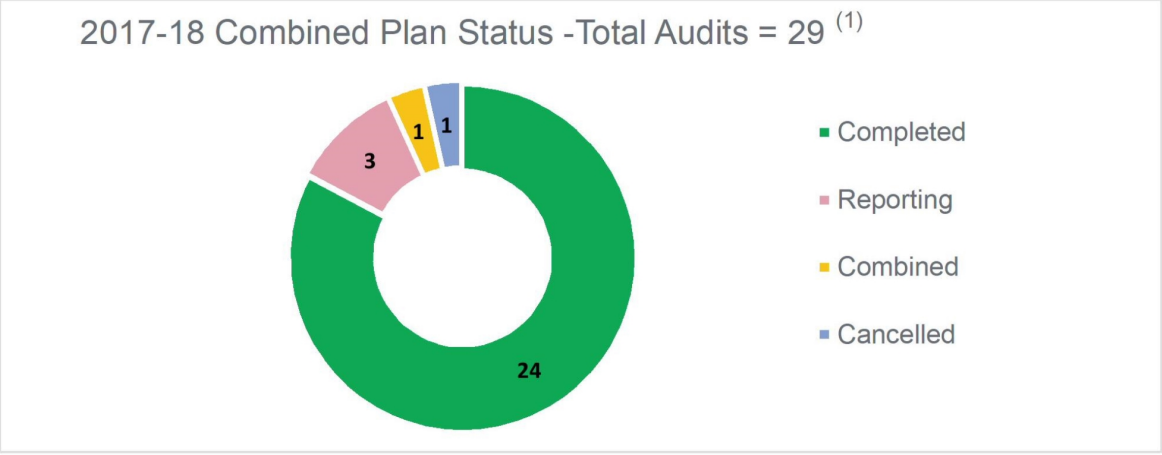
Questions this paper addresses

- 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):

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



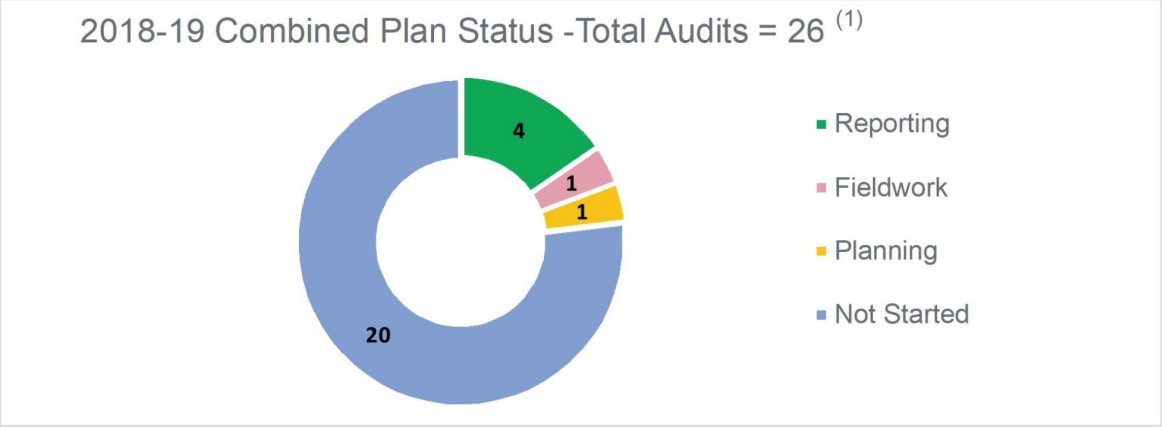
(1)ARC approved baseline plan for 2017-18 (16 internal control reviews & 13 change assurance reviews)

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:

UKGI00021233



(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 20 July 2018):

Audit Action Status:	
Open (not yet due)	29
Overdue (<60 days)	2
Overdue (>60 days)	0
Total	31

More detailed information is provided in paragraphs 11 - 12 of the report.

4. Internal Audit Co-source Appointment:

A separate paper has been submitted to formally request the committee's ratification of the decision to appoint the new internal audit co-source provider.

5. Significant Issues:

Changes arising from the transition to the new Co-Source provider as well as changes to the IA team (Alberto Zanatta has recently tendered notice of his resignation as he has decided to return to Italy) will need to be reviewed in terms of the impact on the deliverability of the plan for 2018-19. We will undertake this review during September as part of the plan refresh and revert to the ARC at its next meeting with recommendations as to any consequential changes proposed.

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

Input Sought

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

UKGI00021233

The Report

Changes to the Audit Plan since May ARC meeting

6. 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.

POMS Audit Plan

7. POL Internal Audit is also responsible for delivery of the audit plan for Post Office Insurance (POMS). Progress with the 2018-19 audit plan is reported at the POMS ARC. Three of the five audits on the plan are in progress:
   - Insurance Distribution Directive (IDD) - readiness review (Reporting)
   - Oversight of Appointed Representatives (Fieldwork)
   - Nemesis Project - Programme assurance (Planning)

Internal audit reviews completed

8. The following four reviews were finalised since the May ARC meeting:
   - IT Governance and Risk Management
   - EUM
   - Branch Technology
   - Business Continuity Management (BCM)

   Below are summaries of these reviews (full reports are available in the Boardpad 'reading room'):

Audit	Key Messages
IT Governance and Risk Management (Ref. 2017/18-19) Needs Improvement ***Sponsor:*** *Rob Houghton* Audit actions: P1: 0 P2: 2 P3: 3 Total: **5**	This review assessed the governance of the programme to implement the IT Controls Framework (ITCF) and the completeness and approach of the IT Risk Transformation deliverables. We conclude that significant progress has been made on establishing an IT controls framework and effective risk management discipline. This is not yet at a business-as-usual state and therefore it has not yet been possible to determine the overall impact on IT governance within the organisation. An audit of the operational effectiveness of the ITCF is scheduled for Q4. We have identified the following key improvements required to the programme: • The next iteration of the programme should improve engagement with key business stakeholders. • Tranche 1 of ITCF implementation (managed by KPMG), lacked effective programme management controls at the time (Nov 2017). Improvements were since made in establishing programme governance processes, however, our opinion is that the tranche 2 plan requires more granular detail to ensure the project is appropriately managed and will be delivered on time and on budget.

UKGI00021233

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 has been 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), at the time of the review (February to May) there were a significant volume of deployments outstanding, specifically 62% of counter terminals had not been deployed. The project team remains confident that deployments can be completed by September 2018, however, this audit has highlighted that there continue to be risks of further cost and delays prior to deployment being completed, with concerns expressed at the time of the review as to whether there was sufficient 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.

UKGI00021233

<table>
<tr><td></td><td>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.</td></tr>
<tr><td>Business Continuity Management (BCM)
(Ref. 2017/18-17)

Needs Significant Improvement

Sponsor:
Jane MacLeod

Audit actions:
<table><tr><td>P1</td><td>0</td></tr><tr><td>P2</td><td>6</td></tr><tr><td>P3</td><td>1</td></tr><tr><td>Total</td><td>7</td></tr></table></td><td>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 BC plans.</td></tr>
</table>

UKGI00021233

Reviews in Progress (2017-18 Audit Plan)

9. 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	Back Office Transformation (POLSAP Migration Re-plan)	Report being reviewed by management

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

10. 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	Nearing completion	30/04 - 15/07
2	Product Risk Review – Postal Orders	Draft report	30/04 – 25/06
3	Employee Expenses	Draft report	14/05 - 15/07
4	Change Governance Framework (Advisory)	Final Draft report	02/05 – 15/07
5	DMB Strategy (Change Assurance)	Draft Report	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

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

Audit Action Status at 20 July 2018:	BAU	Change	Total
Open (not yet due)	19	10	**29**
Overdue (<60 days)	2	0	**2**
Overdue (>60 days)	0	0	**0**
Total	21	10	**31**

UKGI00021233

12. Audit actions are generally being completed on time. The following two actions are currently overdue (less than 30 days) albeit with justifiable reasons:

Description of audit finding and Priority rating	GE owner and due date	Action Owners and Status Update
Information Security Assessment 2016 - follow-up review		
Inadequate usage of data classification and lack of data owners. Action: The GDPR project will address the issue around data owners where personal data is involved.	Jane MacLeod 30/06/2018	*Owner: Somita Yogi* The Retention and Disposal Policy has been finalised. Data classification standard have been developed. The MI & Data Team is progressing with the identification of the Data Owners (the top 6 systems and applications to be in scope have been agreed), however the exercise has not yet been completed. Progress with this action is tracked by the Information Security Committee.
Lack of DLP (Data Leakage Prevention) solution. Action: The IT Security Transformation programme will deploy a Data Leakage Prevention (DLP) solution to identify all confidential documents shared outside of PO.	Rob Houghton 30/06/2018	*Owner: David Meldrum* Data Leakage Prevention controls are in place and being reviewed for technical requirements. A solution for tracking and stopping data leakage has been designed.

END OF REPORT

UKGI00021233

Appendix 1

2017-18 Internal Audit Plan - Status as at 20 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	**Needs Improvement**
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	**Merged**	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).

UKGI00021233

Appendix 2

2018-19 Internal Audit Plan - Status as at 20 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	**Reporting**
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	Q4	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	**Reporting**
2	Payzone Business Integration	D. Smith / A. Cameron	Original	TBC	Not Started
3	DMB Strategy	D. Smith	Original	July	**Reporting**
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).

UKGI00021233

Risk Report

Author: Jenny Ellwood Sponsor: Jane Macleod Meeting date: 31 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 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

a) What are the key risks identified from rolling out the placemat in IT, Identity Services, Communications, HR and Strategy?
b) What are the next steps in embedding the placemat approach?
c) What is the current change portfolio delivery status and key delivery challenges?
d) What are the current top portfolio risks and where are we with the development of the Strategic Portfolio Office and change delivery improvements?
e) 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. We have successfully rolled out the Placemat to all business area, with the final roll-out of the Placemat to IT, Identity Services, Communications, HR, and Strategy this quarter. A full update is shown in paragraphs 9- 14. For IT the rollout provided affirmation that the top risks identified through their existing risk process remained the same. For Identity Services the risks identified were based on early thoughts on strategy and as the proposition

UKGI00021233

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 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 October.

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 23 to 30.

7. There are currently 9 live Risk Exceptions and an update on the key activities for this period is provided in paragraph 35. Also see appendix 1.

Input Sought

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

UKGI00021233

The Report

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

IT

9. 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 October/ February (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) Oct - Feb b) Oct - Feb c) 31 Dec – 28 Feb d) Complete e) Ongoing	6 I/L 3:2

- **Fujitsu Failover Horizon Datacentre Failover Test –** The decommissioning of POLSAP from Fujitsu has moved from September 18 to between October and February 2019. 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	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	6 I/L 3:2

UKGI00021233

Risk Title	Risk	Current RAG	Mitigation Plan	Due date	Target RAG
	losses, reputational damage, and prolonged service interruption.		d) Monthly IT Service Continuity reviews in place.	d) Ongoing	

- **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

Human Resources

10. 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	12 I/L	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

UKGI00021233

	North Star strategy which will be impacted significantly if these key individuals suddenly left the business	**4:3**	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

Identity Services

11. For Identity Services, the risks are reflective of the developing stage for their business. 10 risks have been identified (work is underway to agree mitigations, control owners and dates). For information the top 3 amber risks are:

Risk Title	Risk	RAG	Latest position /Mitigation where agreed
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**	Resource has been brought into the team with the requisite skills and experience to develop an identity proposition and to select appropriate technology supplier to build and create the identity solution.
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 and Information Security	The risk of development and launch of sub-standard products with inadequate DP and IT security. This may result in regulatory action and/or adverse media coverage leading to financial and potential reputational loss	**8** **I/L** **4:2**	a) Design of product will be in line with industry required DP and IT standards b) Appropriate pen and security testing will be undertaken

Strategy and Comms

12. The risks identified by the Comms team are at an operational level with no material ones at this stage.

13. The risks identified by the Strategy team relate to delivery of their responsibilities, as opposed to the strategic risks to Post Office. The latter will be addressed through the Central Risk team work (see paragraph 15). The Strategy team has identified one key amber risk relating to dependence on key personnel. Plans are in place to use interns to capture knowledge to ensure continuity and minimise the impact of a sudden departure of key personnel. This risk is reported through the wider HR key

UKGI00021233

person dependency risk.

14. 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?

15. 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 improving risk and control descriptions, greater consistency into scoring rationale, consolidating principal risks and linking through connected events such as audit findings and risk incidents to;
    - identifying, assessing and managing the strategic risks to Post Office achieving its North Star ambitions and delivering on its strategic priorities;
    - developing executive reporting and oversight on the 'top risks', including reviewing more closely those risks with potential strategic impact;
    - simplifying the risk exceptions process and exploring ways to digitise it in order to provide greater effectiveness and efficiency in raising, approving, monitoring and reporting 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 by 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?

16. 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.

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

UKGI00021233

18. Back Office Transformation has amended its go live date from September 2018 due to 3 issues, delayed interface delivery, high volume system performance issues and cash forecasting algorithm changes. All items are under review and subject to proof points towards the end of July the project will confirm whether a go-live before Christmas change freeze is feasible. Positively the second system integration test (SIT) phase is now complete with far less defects than seen in the first round of SIT and high volume data validation for settlement is already almost 100%. A 3rd party is currently engaged to review our test coverage, reporting back end of July.

19. 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 August 2018. 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?

20. There are two portfolio top risks for ARC to note: i) Risk of increased costs and delayed benefits through the late delivery of Change and ii) EUM effectiveness an update is provided on these from paragraph 30.

21. 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

22. 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.

23. In January 2018, PA Consulting undertook a maturity assessment of the current capability against other organisations operating in the retail and

UKGI00021233

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.

24. 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.



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

26. 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;
    - 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.

27. Phase 1 also includes the development of a prioritised Investment Portfolio for 2018/19, the introduction of One Best Way improvements and

[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.

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

UKGI00021233

enhancements to governance. This includes replacing the existing Change Approvals Group with Change and Portfolio Performance Review Committees to provide better focus.

28. 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	

29. 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.

30. Finally, we have also recently commissioned Deloitte to undertake some separate work on the emerging change assurance model to provide additional assurance that the way forward, and progress against it, is sufficiently comprehensive and robust. A draft status of the report is now with the Strategic Portfolio Director for review and comment.

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: o launched	31/7 31/7 Complete Complete	6 I/L: 2:3

UKGI00021233

Risk Title	Risk	Current RAG	Mitigation Plan	Due date	Target RAG
			○ recruitment completed ○ target operating model phase 1 ○ target operating model phase 2	30/9 30/9 31/3/19	

Enhanced User Management (EUM)

31. 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.

32. 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.

33. 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.

34. 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 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.	**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 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	Complete 12 July 30/7	**9** **I/L: 3:3**

UKGI00021233

Risk Title	Risk	Current RAG	Mitigation Plan	Due date	Target RAG
			over 6000 branches by end of July 18.		

What is the current status of Risk Exceptions?

35. There are 9 approved Risk Exceptions currently in place. For information purposes within appendix 1 we have provided details of 4 exceptions which are either new or have overdue actions we want to make you aware of:
    - 1 RER related to Success Factors has one overdue action relating to the creation of a corporate solution for Single Sign on and Bring your own devices to remove ability for employees who have the access to all employee data being able to access this from external devices. It was anticipated this would have been approved and in place by the end of June but this has not been possible. Work is underway to see if the interim mitigations are appropriate to allow restricted access to continue or whether we need to remove access until a solution is in place.
    - 2 new RERs which were authorised as part of the Customer Hub go live, both of which have approved actions and due dates – neither create high risks to Post Office at present

36. As mentioned in paragraph 15 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.

UKGI00021233

Appendix 1: Risk Exceptions

Title (Type) and Risk	Owner	Date	Actions	Due Date	Status/ Update
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-Joe Arakji (interim) Accountable-Joe Arakji	Raised: 02-Jan-18	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.
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. It's not possible to encrypt the email address /phone number data items since these are the critical fields needed for the search.	GE-Owen Woodley Accountable- Ray Panditharatna	Raise: 01-Jun-18 Close date: 31-Oct-18	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 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	31-Oct-18	**Not yet due.**

UKGI00021233

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 [redacted] Payments. [redacted] 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 [redacted] approval, and as this is a tripartite agreement this poses a significant risk to POL in that [redacted] 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 [redacted] 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 side letter has been updated and is going through review and PO approval, and resolution is imminent.

UKGI00021233

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.

Grounding the Balance Sheet – Protecting the Brand
Driving Shareholder Value

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 results 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 manager… are separate conversations	✓ Risk management is embedded in performance management ✓ Agility in anticipating and responding to issues ✓ Ability to exploit uncertainty to drive value

UKGI00021233

Compliance Report

Author: Jonathan Hill Sponsor: Jane Macleod Meeting date: 31st 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. IRRELEVANT
IRRELEVANT
- 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
- Easy Life sales through CRMs need to see a material improvement in conformance if they are to continue to sell the product. There is a risk of customer detriment if the full question set is not asked. An action plan is in place and is being enhanced
- Meeting the future regulatory agenda. There are a large number of items featured in the regulatory appendix. 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.

UKGI00021233

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

UKGI00021233

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

UKGI00021233

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. POI/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 no issues resulting in material customer detriment were identified at that time. The JCC meets monthly
- Two red metrics (out of 15) were reported and related to:
  - Fulfilment issue: Upheld complaints on 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 since its launch in February 2018. To address this VMS issue, additional training has been

UKGI00021233

provided to the CRMs and their supervisors. The product team, together with Royal London and the Post Office Compliance team are developing improvements to the CRM sales approach, simplifying the application process on the tablets. These changes are being planned to coincide with the IDD changes due in September 2018

- The POI Board (held on 19th July) was advised that, following recent conversations with Royal London (the Easy Life underwriter), there is a risk of material customer detriment if a customer has not been asked to answer all the questions in the application, with particular reference to smoking and cancer questions. If there was not a full disclosure, the underwriter might reject a claim or at least pro rate any claim payment
- Accordingly and together with its on-going concerns about branch sales process conformance, the POI Board expressed concern that unless it sees a material improvement in Mystery Shopping results by the end of the calendar year (including a move to at least amber within the next 3 months) it will consider whether the product should be pulled from distribution through CRMs
- Following the update from Royal London the POI and Post Office Compliance Teams have met and have agreed some immediate next steps, whilst we look at other options to make a step change in conformance:
  a. Brief the sales team on need to improve conformance and set out why this is so important – i.e. the real potential for customer harm
  b. To support the branch team produce a "route to green" plan, which includes embedding a conformance culture, by the end of August 2018
  c. Review withdrawal of sales 'licence' if sales volumes are below a certain frequency (until the CRM can re-prove capability)
  d. POI to work on getting Royal London to accelerate the application changes ahead of the September planned date
  e. Uplift mystery shopping for Easy Life
  f. Contact all Easy Life customers by mail / post-sale call to check they were asked the appropriate questions and establish an action from there to address the risks identified

- The POI Assurance Team has completed a review of the Easy Life implementation processes since the product launch in February 2018 (e.g., initial training, on-going CRM support, first line controls and the quality of sales). It found that, whilst there are always areas for improvement, there were no significant issues

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

UKGI00021233

8. Banking Framework Security Compliance and Governance Committee (SCGC) – meeting held on 6th June at which the following were raised:

- 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 key 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. We are looking to recharge these penalties to the supplier

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

UKGI00021233

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

UKGI00021233

- Annual AML/CTF training for Network and back office staff was delivered 4th – 30th May 2018. As at 12th July completion levels were 97.3% for Network and 96% 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 have now received its written response. 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

- Annual risk assessment work continues and no products assessed to date pose a material risk to the Post Office
- 19 Product Information Packs have been received for Mobile Phone Top Ups, Postal Orders, Travel Money Hub, Partner Banking Framework x9, Bill Payment Pre Paid Cards, Drop and Go, Gift Cards, MoneyGram, Bill Payments,

UKGI00021233

Multi-Currency Card and International Payments. There are no Product Information packs overdue. 7 are due in July and August (PaySafe Cash, Amazon Top-ups, POCA, Business Cheque Encashment, Current Accounts, Savings, Bureau de Change). There have been no major concerns identified within these PIPs

- In May and June, 14 products/projects were supported and their financial crime risks reviewed. This included new products (e.g., Amazon branch top ups), our partner banking framework services and our new travel money app. Whilst a number of comments were made in relation to product specific issues no major Financial Crime risks have been identified
- POI products were due for reassessment in May, however there were no PIPs completed at that time. A workshop was held in May with POI to assist with PIP completion and we are working with them to complete their PIPs

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

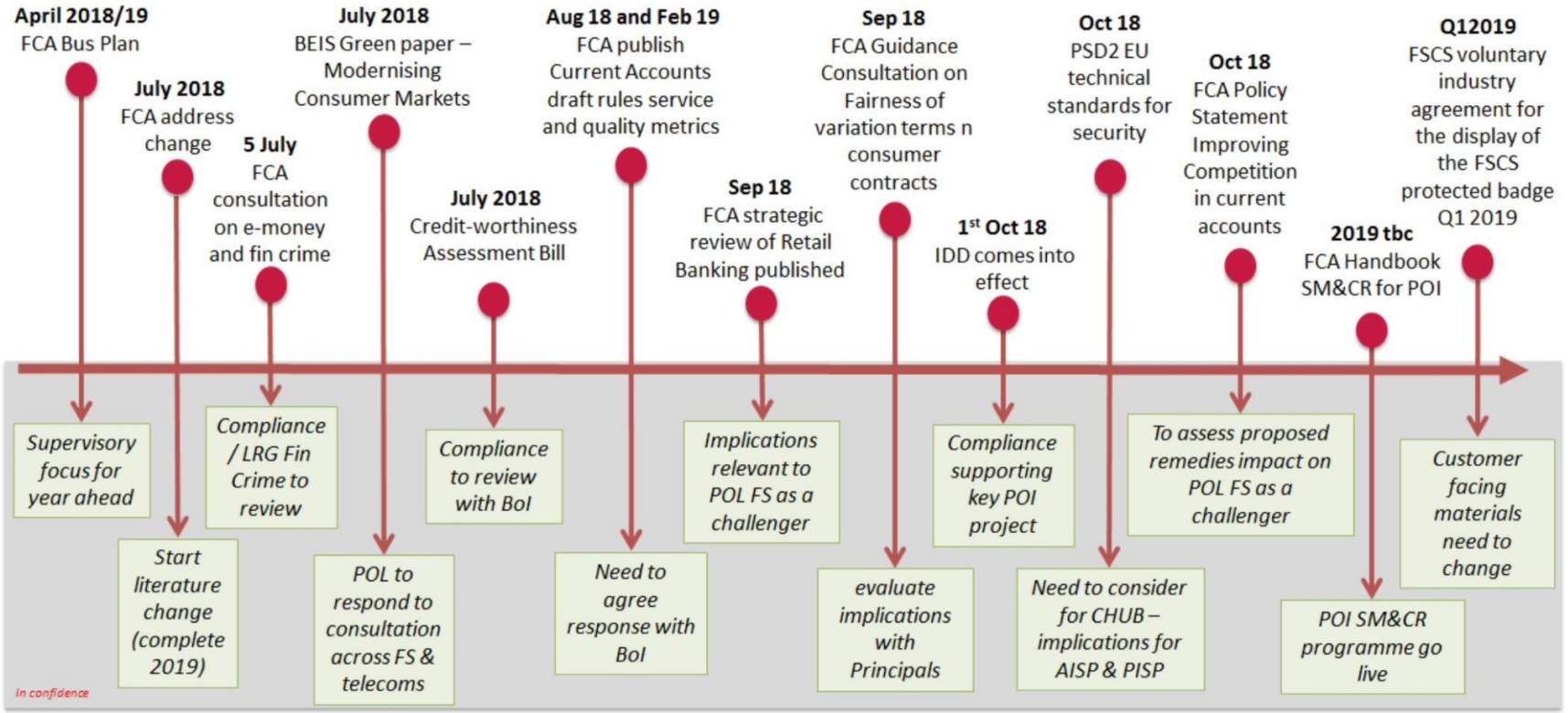
- IRRELEVANT
- This is not a new style of attack, but illustrates that criminals will exploit known modus operandi and system weaknesses

UKGI00021233

What is the forward-looking regulatory agenda?

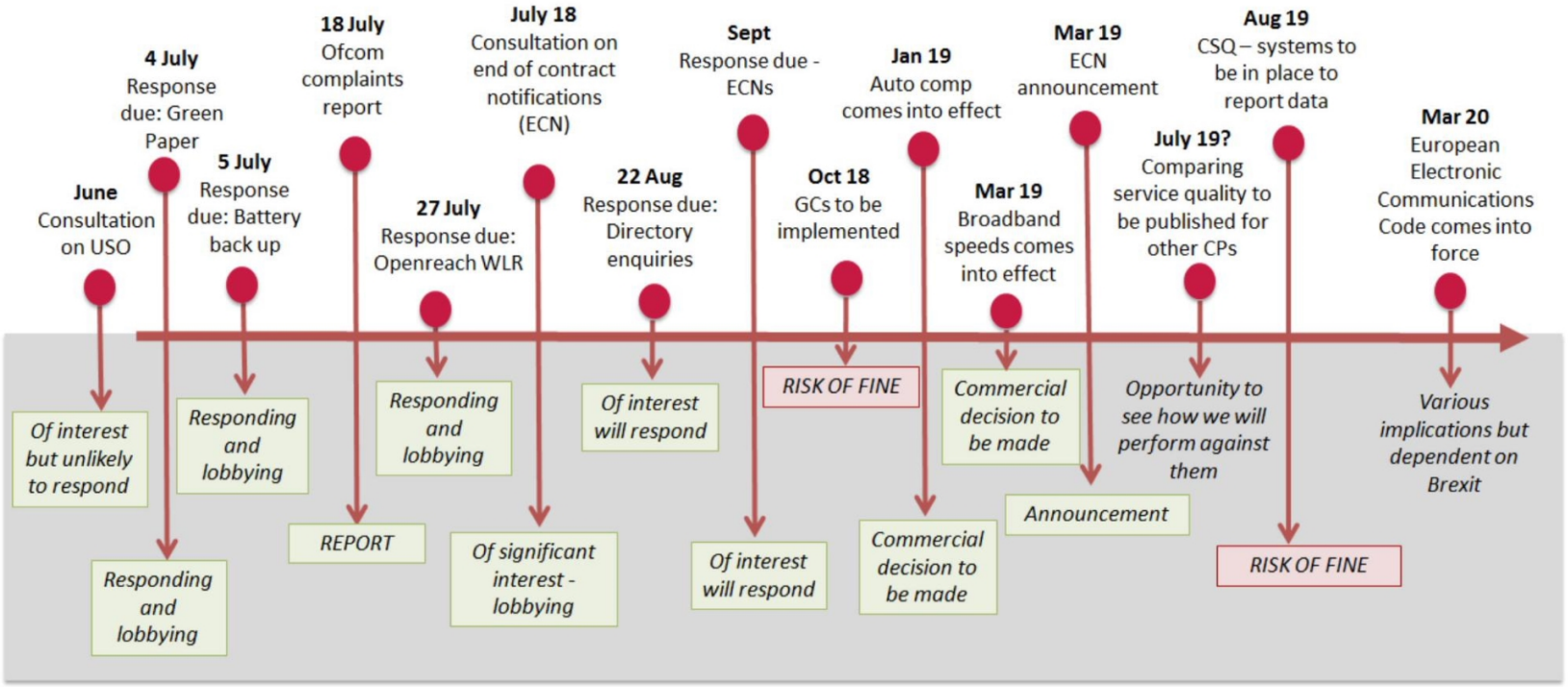
20. The tables below set out the key activities of the Financial Services and Telecoms regulators. As we develop this we will look to include calendars for Financial Crime and Information Security regulation.

Post Office Financial Services Regulatory Calendar



UKGI00021233

Post Office Telecoms Regulatory Calendar



Confidential

UKGI00021233

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

UKGI00021233

POST OFFICE

AUDIT, RISK AND COMPLIANCE COMMITTEE

Vulnerable Customers Risk Assessment and Gap Analysis

Author: Jonathan Hill

Meeting date: 31st 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 2018.
5. Attached in the Appendices are the assessment, the proposed work plan and the approved policy

Questions this paper addresses

6. How wide-ranging is vulnerability in the UK?
7. How are the Government, regulators and business responding?
8. How does Post Office currently look after Vulnerable Customers?
9. What further activities must Post Office undertake to support Vulnerable Customers?

Conclusions

10. 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.
11. The risk assessment has identified some key required improvements as well as some other items that we could take forward.
12. Key items we are taking action on include:
    - Required re-organisation and improvement in providing branch literature in an alternative format to vulnerable customers

UKGI00021233

- 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

13. 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)
14. 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

15. The Government and regulators have put increasing emphasis on ensuring that society does more to ensure that vulnerable customers are protected. For example BEIS produced a green paper on "Modernising Consumer Markets" (April 2018), which states,

UKGI00021233

"*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'."

Ofcom

16. 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.

FCA

17. 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.

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

18. 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)

19. '*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)

20. 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.

21. 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

UKGI00021233

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

22. 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?

23. Overall the work has shown that we can demonstrate that Post Office takes its responsibilities to vulnerable customers seriously. For example,

- Numerous community outreach and partnerships with local charities/vulnerable customers made through Agency branches (e.g., the activities of Pontrillas branch, which established a group to combat loneliness and to visit elderly people at home, as featured in Post Office One)
- 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, with trained staff on hand

UKGI00021233

24. 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 do we need to do?

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

Telecoms Text Relay service

28. 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.

New Ofcom General Condition Requirements

29. 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.

30. 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).

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

Training our staff and the Network (including Dementia Friends)

32. 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.

UKGI00021233

33. We intend to build on this with a specific module on 'vulnerable customers' on Success Factors that will be available for all our employees.

34. 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.

35. 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.

Communication on the Post Office Website

36. 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 BoI.

37. 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

38. 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).

39. 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.

Appendices

Appendix 1: Vulnerable Customer Risk Assessment and Plan
Appendix 2: Vulnerable Customer Work Plan
Appendix 3: Vulnerable Customer Policy (Approved September 2017) – Available in the BoardPad Reading Room)

Jonathan Hill
Director of Compliance

UKGI00021233

Vulnerable Customers

Assessment of approach towards 'Vulnerable Customers'

13/07/18

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

UKGI00021233

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**
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 (Sep 2018)**

UKGI00021233

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. This is a suggested action to be considered by gating team/SLT	**TBC**	**To be agreed**

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. This report is very supportive. PO to review and consider if there are any lessons learned as a result of this,
				Green	**Network to review and follow up with mails team as BAU**

UKGI00021233

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 else's 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:	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	**Amber**	**Ross Borkett** **Pilot Q4** **Launch Q1 2019/20**

UKGI00021233

Vulnerable Customers

Which areas	What we know (how we support customers)	Reg/Legal Regt	Suggested actions	RAG Status	By Who (Owner)
	• Braille • Large print • Audio CD		pressure on traditional high 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.		

UKGI00021233

Vulnerable Customers

Which areas	What we know (how we support customers)	Reg/Legal Regt	Suggested actions	RAG Status	By Who (Owner)
			• Deliver a sustainable profit. • 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	**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	**Green**	

UKGI00021233

Vulnerable Customers

Which areas	What we know (how we support customers)	Reg/Legal Regt	Suggested actions	RAG Status	By Who (Owner)
	provide additional 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		'Vulnerability Charter' to build on existing commitments 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	**Green**	**Bryn Robertson Morgan Ongoing Programme through to 2019**

UKGI00021233

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.		scope for sharing a central ID standard.		
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**

UKGI00021233

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.	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**

UKGI00021233

Vulnerable Customers

Which areas	What we know (how we support customers)	Reg/Legal Regt	Suggested actions	RAG Status	By Who (Owner)
	The regulator has also tacitly acknowledged that its application of 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.	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	**Green**	**PO Money and BoI (March 2019 for third party access initiative)**

UKGI00021233

Vulnerable Customers

Which areas	What we know (how we support customers)	Reg/Legal Regt	Suggested actions	RAG Status	By Who (Owner)
	PO Money Mortgages – specialist team to support customers when faced with ~~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.		the minimum standard. The mandate can also be adjusted 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	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**

UKGI00021233

Vulnerable Customers

Which areas	What we know (how we support customers)	Reg/Legal Regt	Suggested actions	RAG Status	By Who (Owner)
	vulnerable re Romance scams, a Medical emergency or utility refund.				
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	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	**Amber**	**Meredith Sharples Oct 2018**

UKGI00021233

Vulnerable Customers

Which areas	What we know (how we support customers)	Reg/Legal Regt	Suggested actions	RAG Status	By Who (Owner)
	with Local Authorities help, as a result 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)		treatment they 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 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.	**Amber**	**Meredith Sharples Need to agree timescales with Fujitsu but likely to be weeks rather than months**
Customer Hub	This important innovation needs to take into account the needs of	Yes (FCA) WCAG	New customer hub. User testing will includes all kinds of	**Green**	**Henk Van Hulle. Sep 2018**

UKGI00021233

Vulnerable Customers

Which areas	What we know (how we support customers)	Reg/Legal Regt	Suggested actions	RAG Status	By Who (Owner)
	vulnerable customers. Whilst many 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.		user testing including those 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**

UKGI00021233

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 and Comms team September 2018**

UKGI00021233

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** **Sep 2018**
	Written Materials/brochures **Communication Materials**	Yes (FCA)(Ofcom) Equality Act	FS&T risk will drive a project plan working with product managers, owners.	**Red**	**Product Owners in FS&T and Marketing**

UKGI00021233

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, Savings,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. Network 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. <u>Customer Relationship Managers</u> 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** **Sep 2018**

UKGI00021233

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.		

UKGI00021233

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**	

UKGI00021233

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**

UKGI00021233

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					

UKGI00021233

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

UKGI00021233

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 Sep 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**

UKGI00021233

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	**Within budgets**	**Meredith Sharples Oct 2018**

UKGI00021233

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 (but expected in next few weeks)**

UKGI00021233

Vulnerable Customers work plan

Which areas	Summary Detail	Reg/Legal Regt	Work plan	Is there a budget consideration?	By Who (Owner)
Communication	**PO Website** **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.	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.	**Not known**	**Rob Wemys Sep 2018**
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	**Within existing budgets**	**Andrew Ellis PO Money Sep 2018**

UKGI00021233

Vulnerable Customers work plan

Which areas	Summary Detail	Reg/Legal Regt	Work plan	Is there a budget consideration?	By Who (Owner)
			avoiding scams, 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, Savings, Pre Paid Funeral, Home	Yes (FCA)(Ofcom) (Equality Act)	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	**Yes, to be determined by solution that needs to be put in place.**	**Product Owners in FS&T and Marketing** **Sep 2018**

UKGI00021233

Vulnerable Customers work plan

Which areas	Summary Detail	Reg/Legal Regt	Work plan	Is there a budget consideration?	By Who (Owner)
	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		vulnerable customers in alternative format 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**	**Paul Beaumont FS&T Compliance Sep 2018**

UKGI00021233

Vulnerable Customers work plan

Which areas	Summary Detail	Reg/Legal Regt	Work plan	Is there a budget consideration	By Who (Owner)
				accommodate 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** **Sep 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** **Sep 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	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**

UKGI00021233

Vulnerable Customers work plan

illness, or 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 **Oct 2018**

UKGI00021233

Whistleblowing Annual Report 2017-18

Author: Sally Smith | Sponsor: Jane MacLeod | Meeting Date: 31st 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 ARC are asked to note the contents of this report.

UKGI00021233

The Report

Summary of activities relating to Whistleblowing reporting 2017-18

1. 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.
2. Training and guidance has been 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.
3. 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.
4. The Speak Up service was promoted through both Paula's blog and the February 2018 Team Talk Plus.

Summary of Whistleblowing reports received 2017-18

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

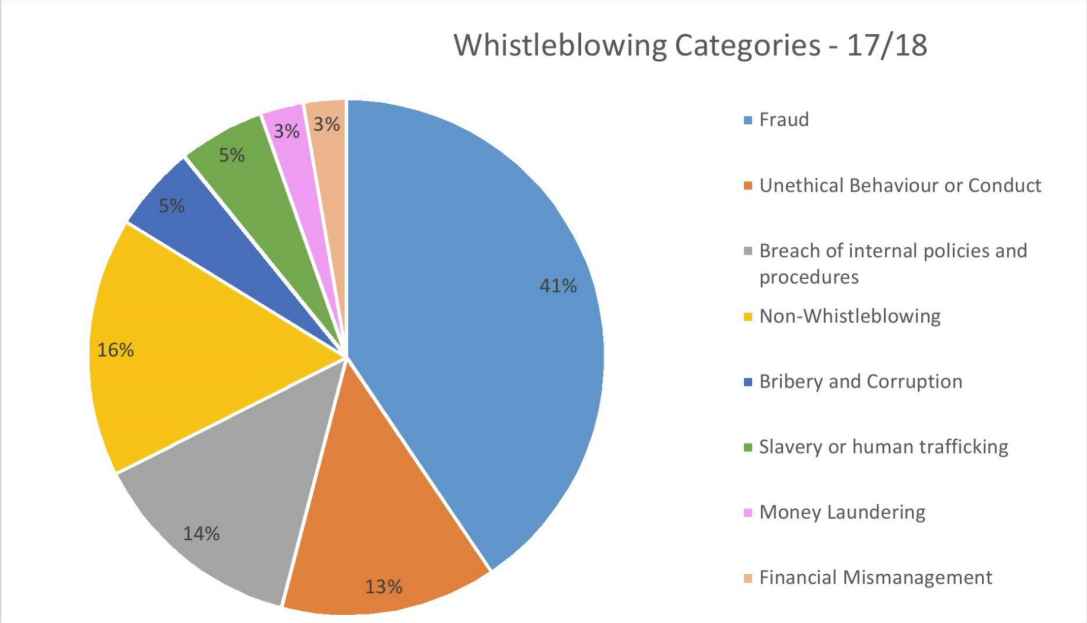
Allegations reported by 2017/18	Volume
Anonymous	10
Postmaster	9
Agent Assistant	6
Unknown	4
Direct Employee	3
Third Party*	3
Member of the public	2

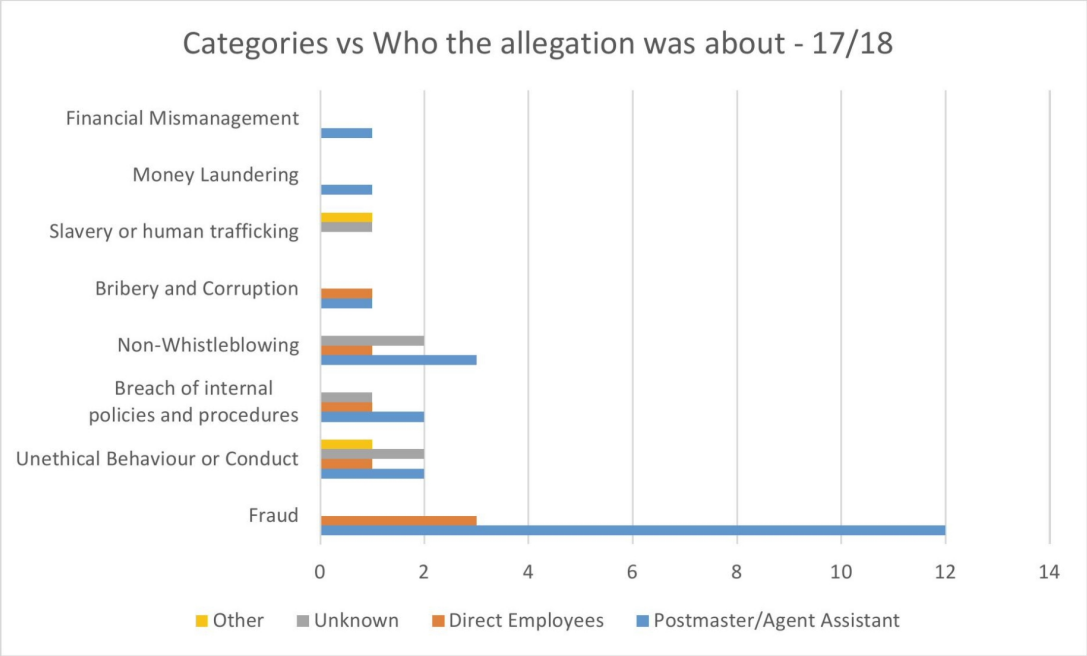
*This includes the Police, Royal Mail and Bank of Ireland

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

UKGI00021233

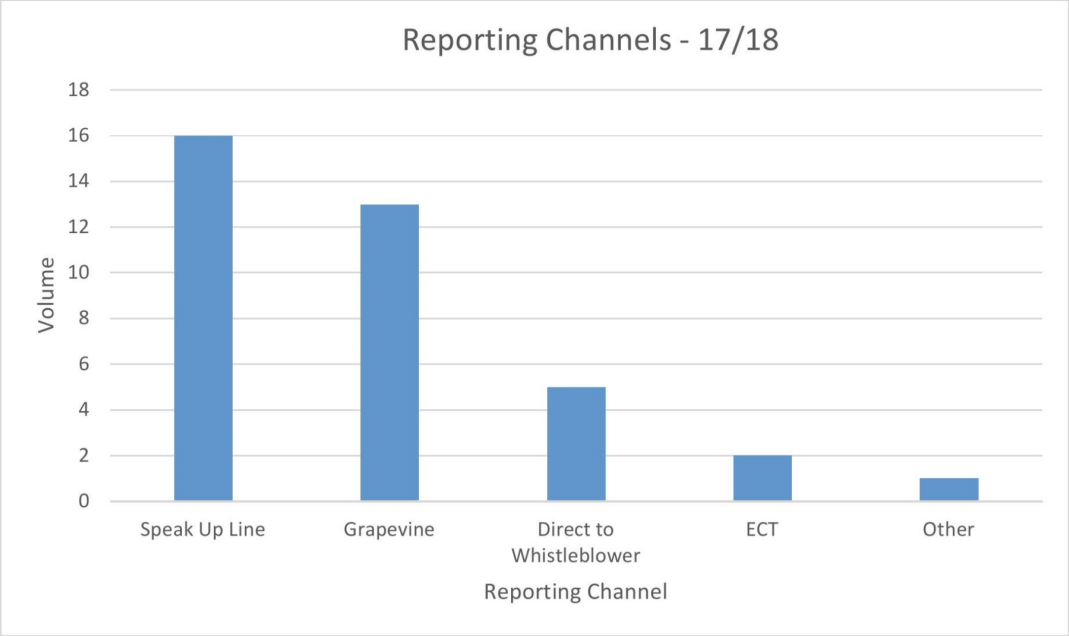
7. 41% of the reports received were allegations of fraud. Predominately this was about either a Postmaster or Agent Assistant (12), however, there were 3 reports involving Post Office employees.





UKGI00021233

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



9. The whistleblowing reports have not identified any root 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:

10. 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.
11. The following activity is planned:
    - Continuous communications and awareness.
    - Whistleblowing Policy annual review and update July 2018
    - Process documents across all areas to be reviewed and updated as required.

UKGI00021233

Gifts & Hospitality Annual Review 2017-18

Author: Sally Smith | Sponsor: Jane MacLeod | Meeting Date: 31st 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. We have not identified any instances indicative of Bribery or Corruption, although there have been minor policy breaches in relation to gifts and hospitality approval.

2. The 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 ARC is asked to note this.

UKGI00021233

The Report

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

1. The new reporting tool, together with user instructions was delivered in August 2017
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:
    - 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. Appendix A shows a summary from the new Gifts & Hospitality reporting tool showing the number of individuals and value (data prior to this is not robust in relation to the number of individuals as not all reports included this data)
7. Whilst an improvement has been seen, it is believed that there is still significant under-reporting, particularly relating to gifts and declined offers.
8. 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.
9. A review of the external companies that have offered hospitality to Post Office in 2017/18 has not identified any significant issues.

UKGI00021233

Planned actions to address issues:

10. The following activities are planned to improve the quality and effectiveness of gifts and hospitality reporting and approval:
    - The minimum control standards in the ABC policy document have been refined
    - 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

UKGI00021233

Appendix A

Gifts and Hospitality for 7th August 2017 to 31st March 2018

Business Area	Gifts Offered		Gifts Received		Hospitality Offered		Hospitality Received	
	Total Value	No. of Individuals	Total Value	No. of Individuals	Total Value	No. of Individuals	Total Value	No. of Individuals
Communication, Brand & Corporate Affairs	£0.00	0	£35.00		£1,300.00	6	£234.00	1
Finance and Operations	£317.00	4	£194.00	3	£2,678.00	13	£2,984.00	14
Financial Services and Telecoms	£0.00	0	£180.00	6	£1,027.07	15	£4,196.00	40
HR	£0.00	0	£0.00	0	£0.00	0	£625.00	6
IT	£0.00	0	£0.00	0	£365.00	5	£34.00	1
Legal, Risk and Governance	£0.00	0	£130.00	5	£1,980.00	43	£9,418.00	84
Retail	£0.00	0	£605.00	31	£1,117.00	13	£770.00	11
Strategy	£0.00	0	£0.00	0	£100.00	1	£0.00	0
Grand Total	**£317.00**	**4**	**£1,144.00**	**45**	**£8,567.07**	**96**	**£18,261.00**	**156**

UKGI00021233

Anti-Bribery and Anti-Corruption Policy

Author: Sally Smith Sponsor: Jane MacLeod Meeting Date: 31st July 2018

Executive Summary

Context

The Audit & Risk Committee (ARC) approved the Anti-Bribery and Anti-Corruption (ABC) Policy in September 2017. The Policy anticipates that it will be reviewed annually. As a result of this annual review, changes have been made which require the approval of the ARC. These changes were reviewed and approved at the Risk & Compliance Committee (R&CC) on 10th July 2018.

Questions addressed in this paper

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

Conclusion

1. Overall, the ABC Policy minimum control standards have been effectively applied since it was last approved, and some assessed as partially effective are being addressed through improved training and awareness.
2. 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.
3. The updated Policy reflects queries and issues received by the Financial Crime team over the last 12 months.

Input Sought

The ARC is asked to approve the updated ABC Policy.

UKGI00021233

The Report

Why do we need to review this Policy?

4. The terms of the Policy require it be reviewed annually.

What changes to the Policy do we propose and why?

5. There have been no legislation changes in the past year and no significant amends made to the policy at this annual review.
6. Minor amends have been made in relation to:
    - 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

What are the implications of these changes?

7. The policy assurance work undertaken in 2017/18 has evidenced that there are some minor failures to apply minimum control standards for Gifts & Hospitality reporting and approval and therefore the controls have been clarified in the updated policy. There are no material changes required to comply with the updated policy
8. Changes to the policy will be communicated to all employees through internal communications which will include a link to the updated document on the Post Office Intranet. Enhanced annual ABC training is being delivered to employees July 2018.
9. The Financial Crime team will continue to monitor adherence to the minimum control standards set out in the policy on an on-going basis and any control gaps identified will be reported to the R&CC and ARC as required.

What will the impact be on our wider business?

10. Public transparency of Post Office's adherence and commitment to ABC will be demonstrated through the publication of the simplified ABC Policy
11. Reinforcement that the failure to comply with the requirements of ABC Policy by any employee will be regarded as a significant breach and may lead to disciplinary action up to and including dismissal and possible prosecution.

What would the impact be of delaying approval?

12. Risk of breaches the Bribery Act 2010 by not having up to date policies and procedures to prevent bribery by any person or company operating on our behalf.
13. Post Office Limited is required to maintain up to date policies to support contractual requirements with clients and suppliers (e.g. MoneyGram and the Banking Framework Services) and failure to do so may result in a breach of contract, and whilst not material, could have commercial and reputational impacts.
14. 'Group' policies such as the ABC Policy are also applicable to Post Office Management Services Limited ('POMS'). 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.

UKGI00021233

Whistleblowing Policy

Author: Sally Smith Sponsor: Jane MacLeod Meeting Date: 31st July 2018

Executive Summary

Context

The ARC approved the Whistleblowing Policy in September 2017. The Policy anticipates that it will be reviewed annually. As a result of this annual review, changes have been made which require the approval of the Audit & Risk Committee. These changes were reviewed and approved at the Risk & Compliance Committee on 10th July 2018.

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 Whistle Blowing Policy minimum control standards have been effectively applied since it was last approved.
2. At annual review, the Whistleblowing Policy has been amended to clarify some minimum control standards, roles and responsibilities
3. There are some minor changes to the requirements and minimum standards of controls which will be communicated to relevant stakeholders

Input Sought

The ARC is asked to approve the updated Whistleblowing Policy.

UKGI00021233

The Report

Why do we need to review this Policy?

4. 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?

5. There have been no legislation changes in the past year and no significant amends made to the policy at this annual review.
6. 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

What are the implications of these changes?

7. The policy assurance work undertaken in 2017/18 has evidenced that minimum control standards are being complied with and no material changes are required to comply with this updated Policy.
8. 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?

9. Transparency of Post Office's adherence and commitment to the Employment Rights Act 1996 and the Public Interest Disclosure Act 1998

What would the impact be of delaying approval?

10. 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.
11. 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.
12. 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.

UKGI00021233

PCI Compliance Status Update

Authors: Mick Mitchell Sponsor: Rob Houghton Meeting Date: 31 July 2018

Executive Summary

Context

Post Office (PO) have not yet achieved a Report on Compliance (RoC) from our external qualified security assessors (QSA), proving our compliance to the Payment Card Industry-Data Security Standard (PCI-DSS). The previous RoC expired on 28th December 2017 and we continue to share our remediation plans with Global Payments (GP), our acquirer, who supports of our plans. We continue to work with the QSA, and our stakeholders, to initiate a strategic and robust regime of compliance going forwards.

Questions this paper addresses

1. What actions are PO taking to address the current situation?
2. Is there an alternative strategic way forward?
3. What is the business impact of this alternative approach?

Conclusion

- PO are progressing remediation activities that are being tracked to complete by end of 2018. However, these 'tactical' remediations are proving difficult to complete due to the current design employed in handling card data, which is proving increasingly costly, complex and has underlying commercial issues requiring resolution prior to a RoC being achieved.
- PO propose initiating a strategic PCI-DSS solution, which does not store card data on the device to resolve the underlying issue of achieving PCI-DSS compliance over the longer term, which was always intended to be implemented post completion of the Network and Branch Counter replacement programmes. Whilst this strategic solution is being put in place, PO will limit tactical remediation until the strategic solution is understood to ensure these activities do not further compromise the end strategic solution.
- The proposed approach will limit the ability of achieving full RoC status until the strategic solution is in place. All stakeholders (the QSA, Partners and Clients) are comfortable that the current non-compliances are not security related but compliance related. PO will continue to keep all stakeholders abreast of progress of the remediation activities and the strategic development to ensure the risk of sanctions against PO remains low. Details of the strategic plan will be presented at the next ARC.

UKGI00021233

Input Sought

ARC is requested to acknowledge support for a more strategic approach to PCI-DSS compliance subject to PO adequately scoping this Programme of work, whilst completing the tactical remediation activities.

Report

What actions are PO taking to address the current situation?

1. 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 (CC) and Fujitsu (FJ).
    a. Within the above, there are 8-10 "project items" that would require the implementation of new systems and ways of working across Computacenter and Fujitsu.
    b. Initial discussions with both CC and FJ have proved complex and timescales to complete new systems implementation and process review could take up to 6 months, with costs ranging from £3-5m. The QSA identified a risk that having 8 new systems to audit annually would not improve PO's opportunity for PCI-DSS compliance.
2. 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.
3. There are a number Change Requests 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.
4. 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 being made.
5. The proposed technical solutions will need to be applied across our entire estate before the QSA can start their re-assessment and accordingly the Steering Group has agreed with QSA's recommendation to recommence the audit post completion of the remedial actions.

Is there an alternative strategic way forward?

6. The PO PCI-DSS estate is increasing over time (the Post Office Data Gateway (PODG) is now in scope, Customer Hub and Panther), although some of these will be covered by separate certifications, not linked with our current PCI-DSS audit.
7. Customer Hub has successfully been launched and we have successfully attained PCI Certification.

UKGI00021233

8. POL have taken the opportunity to review the POL Business & IT Project Portfolio and have identified a number of Projects that would improve PO's ability to achieve a more permanent PCI–DSS solution and RoC status. These include the Belfast Data Centre Exit of Horizon Applications into a Fujitsu Serviced Azure Cloud and the Retail strategy to replace end of life Pin Pads over the next two financial years. The results of these projects combined would provide a better, more routine maintainable and robust PCI – DSS compliant position than the current tactical remediation activities.

9. 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.

10. This approach will require investment and time to implement (possibly 12-18 months). Nicholas Spicer and his team within Payment Services are compiling a business case for a possible solution.

11. 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.

What is the business impact of this alternative approach?

12. This alternative approach will mean that full RoC status is not achieved until the longer term strategic solution is put in place. However, we will continue to ensure all new solutions are RoC compliant and aligned with the strategic direction of not holding card data on devices (e.g. Customer Hub has achieved RoC status).

13. 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.

14. The Banks ultimate sanction is to terminate their part of the agreement, although we believe this is a very low risk and PO would have a significant time to recover once any formal notice was issued.

15. 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.

16. 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.