POL00423570

POST OFFICE LIMITED

Meeting:	Risk and Compliance Committee
Date:	13 July 2020
Time:	14.00 - 17.00
Location:	Via Microsoft Teams

Present:	**Attendees:**
Alisdair Cameron (Chairman)	Johann Appel (Head of Internal Audit)
Ben Foat (Group General Counsel)	Mark Baldock (Head of Risk)
Amanda Jones (Group Retail and Franchise Network Director, Interim)	Jonathan Hill (Compliance Director)
Chrysanthy Pispinis (deputising for Owen Woodley)	Tom Lee (Head of Finance Financial Accounting and Controls)
Lisa Cherry (Group Chief People Officer)	David Parry (Senior Assistant Company Secretary)
Jeff Smyth (Group Chief Information Officer, Interim)	Tony Jowett (Chief Information Security Officer): Item 4
Julie Thomas (Operations Director)	Joseph Moussalli (Programme Manager): Item 4
	Rob Wilkins (Cloud Services Director): Item 4
	Tim Armit (Business Continuity Manager): Item 5
	Maxine Cross (Head of Reward and Pensions): Item 7
	Tim Perkins (Head of Security, Safety & Loss Prevention): Item 8
	Sarah Gray (Group Legal Director): Item 9
	Barbara Brannon (Procurement Director): Item 10
	Andy Kingham (Head of Network): Item 11
	Sally Smith (MLRO & Head of Financial Crime): Item 11
Apologies:	
Nick Read (Group CEO)	
Owen Woodley (Group Chief Commercial Officer)	
Dial In Details:	
Join Microsoft Teams Meeting GRO United Kingdom, London (Toll) Conference ID: GRO Pin (if applicable): GRO	

Time		Item	Owner	Action
14:00	1.	Welcome & Conflicts of Interest	Chairman	Noting
14.05	2.	Previous Meetings	Chairman	
		2.1 Minutes (6 May 2020)		Approval
		2.2 Action List		Discussion
14.10	3.	Combined Risk, Compliance and Audit Update		
14.10		3.1 Risk Report	Mark Baldock	Noting (onward submission to ARC)
14.25		3.2 Compliance Report	Jonathan Hill	Noting (onward submission to ARC)
14.40		3.3 Internal Audit Report	Johann Appel	Noting (onward submission to ARC)
14.55	4.	PCI-DSS and Cyber Security Update	Jeff Smyth/ Tony Jowett	Noting (onward submission to ARC)
		4.1 PCI-DSS	Jeff Smyth	
		4.2 Cyber Security	Tony Jowett	
		4.3 Joiners, movers, leavers	Tony Jowett	
15.10	5.	Business Continuity Update and Business Continuity Policy	Tim Armit	Noting & Approval (onward submission to ARC)

Strictly Confidential

POL00423570

POST OFFICE LIMITED

15.20	6.	GDPR Update	Jonathan Hill	Noting (onward submission to ARC)
15.30	7.	Pensions Assurance – RM Pensions	Maxine Cross	Noting (onward submission to ARC)
15.45	8.	Suspense Accounts	Tim Perkins/ Ben Foat	Noting (onward submission to ARC)
16.00	9.	Law & Trends Update	Sarah Gray/ Ben Foat	Noting (onward submission to ARC)
16.10	10.	Procurement Governance & Compliance Report	Barbara Brannon	Noting (onward submission to ARC)
16.20	11.	Policies for Approval:	Jonathan Hill	Noting (onward submission to ARC)
16.20		1. Modern Slavery Statement	Andy Kingham (see item 5)	
16.30		2. Business Continuity Policy	Sally Smith	
		3. Anti-Bribery Corruption Policy	Sally Smith	
		4. Whistleblowing Policy		
		5. Financial Crime Policy		
		6. Anti-Money Laundering and Counter Terrorist Financing Policy		
		7. Document Retention Policy		
		8. Procurement Policy		
16.50	12.	Review of draft Audit, Risk and Compliance Committee (ARC) meeting agenda 27 July 2020	Chairman	Noting
16.55	13.	Any other business	Chairman	Noting

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

Strictly Confidential

POL00423570

2

POST OFFICE LIMITED
RISK AND COMPLIANCE COMMITTEE
Minutes of a Risk and Compliance Committee ("RCC") meeting held via Microsoft Teams
on 06 May 2020 at 14:00

Present:	Alisdair Cameron (Chair) (AC)	Group Chief Financial Officer	
	Ben Foat (BF)	Group General Counsel	
	Amanda Jones (AJ)	Group Retail and Franchise Network Director, Interim	
	Lisa Cherry (LC)	Group Chief People Officer.	
	Jeff Smyth (JS)	Group Chief Information Officer, Interim	
	Julie Thomas (JT)	Operations Director	
	Andrew Goddard (AG)	Payment Propositions Director (deputising for Owen Woodley)	
In Attendance:	Johann Appel (JA)	Head of Internal Audit	
	Mark Baldock (MB)	Head of Risk	
	Jonathan Hill (JH)	Compliance Director	
	Tom Lee (TL)	Head of Finance, Financial Accounting and Controls	
	Rebecca Whibley (RW)	Assistant Company Secretary	
	Tony Jowett (TJ)	Chief Information Security Officer	Item 5
	Sherrill Taggart (ST)	Legal Director, Interim	Items 6 & 7
	Barbara Brannon (BB)	Procurement Director	Item 8
	Rod Williams (RW)	Head of Legal, Dispute Resolution & Brand	Item 9
Apologies	Nick Read, Group CEO		
	Owen Woodley, Group Chief Commercial Officer		

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

1.1 The Chair opened the meeting and advised that all papers would be taken as read. No conflicts of interest were declared.
AC noted there were four issues that were being managed under legal supervision and which would be discussed at ARC:

1. An independent review of suspense accounts as part of the GLO work;
2. An independent review on stamps and whether there were GLO implications;
3. A CBRE performance issue that had been uncovered; and
4. Work ongoing to validate historical final salaries for the defined benefit pension scheme.

2. Minutes and Action Lists

2.1 The minutes of the RCC meeting held 9 March 2020 were **APPROVED**.

2.2 Progress on completion of actions as shown on the action log was **NOTED** and the actions assigned to SH (Shikha Hornsey) were to be reassigned to JS. The following action updates were provided: **To do: RW**

- Action 3.3 from 14 March 2020 relating to FRES Audit would be completed before the next RCC and the action remained **open**.
- Action 3.3 from 4 March 2020 relating to guidance from the National Cyber Security Centre was **closed**, the guidance having been shared with the Group Executive (GE) and Board.
- Action 4.12 from 14 March relating to the Ofcom Information Requests was **closed**.
- Action 6.6 from 14 March relating to the issues being flagged to the RCC or ARC was questioned as to its context and it was requested that more information was provided as it was not enough to simply say that it was not raised. The action remained **open**. **RW**
- Action 6.18 from 14 January 2020 relating to Payment Services Directive was **closed**.
- Action 10.6 from 14 January 2020 relating to Money Laundering Reporting Officer (MLRO) Annual Report had been delayed due to scheduled meetings being postponed. The action remained **open**.
- Action 3.2 from 7 November 2019 relating to supplier contracts out of governance (SSK) remained **open**.
- Action 3.3 from 7 November 2019 relating to supplier contracts out of governance (Brands/RAPP) remained **open**.

POL00423570

- Action 4.1 from 7 November 2019 relating to the PCI-DSS Update and final pricing deadlines from Ingencio was **closed** as this item had become a regular RCC agenda item. **JS**
- Action 5.3 from 7 November 2019 relating to major incident testing remained **open** and JS advised he would obtain an update.
- Action 5.3 from 7 November 2019 relating to Joiners/Movers/Leavers and third party access remained **open** and TS was asked to provide an update.
- The following actions from 7 November 2019 were otherwise **closed**: 5.3 Cyber Security relating to Joiners/movers/leavers and the contract review, 5.3 Cyber Security relating to Joiners/movers/leavers being added to the Internal Audit Plan, 6.14 relating to Data and Analytics Excellence (Programme Assurance) and 7.5 relating to Contracts Management Framework.
- Action 5 from 3 September 2019 relating to GDPR was **closed** as JH advised that contracts had been identified and the GDPR programme was due to be completed at the end of June 2020.

3. Combined Risk, Compliance and Audit Update

Risk

3.1 MB explained that since the last RCC on 14 March 2020, his team's focus has been on the COVID-19 crisis and fortnightly risk updates were being provided to the COVID-19 SteerCo, which was included in the paper to the RCC. This work had been undertaken in two phases. The first was to undertake the industry-wide and sectorial analysis of the typical emerging COVID-19 risks and was completed by 31 March 2020. The second phase was to discuss the risks that had been identified with the business to confirm relevance and to assess their respective impacts, likelihood and proximity. It was concluded that there was one single overarching COVID-19 enterprise risk, 13 intermediate thematic risks (operational, strategy, legal, financial etc.) and 56 specific low level risks. One major risk was having insufficient change funding available to deliver planned change activity and it as noted that this was due to be discussed at the Board.

3.2 Work was now moving to merge existing risk work with the COVID-19 risks due to the wide scope of these risks. The team was also continuing to implement Archer and MB explained that all risks were due to be entered into Archer by the end of next week (15 May 2020) and the system was to be rolled out to the wider business from 31 May 2020.

3.3 MB also highlighted that his team had produced a risk appetite statement for COVID-19, but that this had evolved into a wider enterprise risk statement and he would be requesting that this statement be considered at the GE in June 2020 (MB to request a GE agenda slot with Veronica Branton, Company Secretary). **MB**

Compliance

3.4 **Telecoms**: JH noted that the regulators have indicated they would not be stepping back from compliance but were being more understanding on the timing for compliance. As an update to the paper, JH explained that his team were now required to provide a weekly update to Ofcom as to our COVID-19 response and they have indicated they are happy with our progress as we are able to do the end of contract notifications, which other providers are still having issues with. Further, we have also just signed up to the Department of Culture, Media and Sport's (DCMS) commitments, including free and low cost calls for vulnerable customers, working with customers who may be struggling with debt and removal of data caps. A statement via DCMS would be released over the weekend. In response to a question from the Chair, JH and AG confirmed (having checked with Meredith Sharples) that there was no financial impact arising from vulnerable customers being unable to pay their bill.

3.5 **PSD2**: JH explained that Fujitsu had now confirmed that they will put in place a fully compliant solution but this would not be the most expensive solution by the beginning of August 2020. There would be a minimal increase in cost, but this was a regulatory requirement. Once in place, we could then apply for an Electronic Communications Exemption (ECE), although we were not being chased to do this.

3.6 **European Electronic Communications Code (EECC)**: JH noted that this would impose new regulatory obligations on all providers. It presented a big challenge for Post Office and had cost implications. Clarity as to what was required was expected from Ofcom but that the DCMS has indicated that it expected providers to meet the implementation deadline of 21 December 2020. The concern was that any clarity from Ofcom may come after this deadline, but it was hoped there may be some leeway. Al noted that if clarity was not forthcoming, we could approach the Department of Business, Energy and Industrial Strategy (BEIS) to support us in seeking this clarity and/or asking for leeway on the implementation deadline. It was also noted that similar changes made to the switching process in the energy industry by Ofgem had led to less switching of providers by customer and therefore there could be retention opportunities for Post Office.

POL00423570

3.7 **Branch Registration Fees:** JH explained that Her Majesty's Revenue and Customs (HMRC) have confirmed that we could defer payment for Branch Registration fees (amounting to circa £3m) until 1 December 2020 (from 30 June 2020). However they have advised that they would calculate the fee based on the June branch data, rather than the December data. This does not go far enough and we would continue to lobby against the decision via BEIS, Her Majesty's Treasury (HMT) and HMRC directly to get HMRC to allow the calculation to apply from 1 December 2020. It was hoped that a positive response would be received soon.

3.8 **Cookies**: JH confirmed he was speaking to Henk van Hulle to try and achieve quicker and cheaper compliance.

3.9 **Belfast Data Centre Exist and move to the Cloud**: The Chair questioned who was having the client conversations and it was highlighted that there should be engagement with client management owners. JH was asked to pick this up with the Commercial team and JS was asked to check with the IT Project Team. **JH/JS**

3.10 **Whistleblowing**: The Chair asked that he was provided with information as to the kind of issues that were being raised by whistleblowers, insofar as it would not breach any confidences. He also questioned whether it was appropriate to be putting investigations on hold. JH explained that these investigations had been put on hold as they required the physical movement of people which was not possible during lockdown. The Chair requested that the investigations were reviewed on a case-by-case basis with HR and challenge the assumption that the investigation had to be paused. If a major issue was subject to the complaint, the response needed to be balanced. **JH** **JH**

3.11 **External Threats – Lottery:** The Chair questioned the wording regarding the Post Office provision of the Lottery having been previously assessed as low risk and JH confirmed that it had been assessed and no issues had been identified. Payzone services were yet to be assessed but AG explained that he did not view it as high risk. The wording of the section would be reviewed before submission to the Audit, Risk and Compliance Committee (ARC) so that it was clearer. **JH**

3.12 **Dangerous Goods**: The Chair noted that overall performance for P12 had dropped to 46% and therefore had got worse. However the Voice of the Customer survey suggested that the question was being asked 75% of the time. IT was noted that the Board may be concerned about the risk of low compliance in this area. Amanda explained that a project had been initiated to place the onus on the customer to confirm what was in their parcel via a validation on the Pin Pad (to reflect the SSK process). The Chair requested that this section of the paper be updated prior to submission to the ARC to better outline this project. **JH/AJ**

Internal Audit

3.13 **2019/20 plan progress**: JA explained that the completion of the 2019/20 internal audit programme has progressed well, however, the final five reviews (three in Post Office and two in Post Office Insurance) were postponed in response to COVID-19 and reprioritisation of the Change Portfolio. Five audits were completed since the March ARC meeting, with the last two reports awaiting management comment. These related to branch sales which had been given a "needs improvement" rating, but the issues raised were not contentious and savings products, which has been given a "green" rating. AG was asked to chase the Commercial Team to ensure that management comment was provided as soon as possible to enable the complete reports to be ready for the ARC on 19 May 2020. Otherwise, the 2019/20 plan was complete (except for the reviews postponed due to COVID-19). **AG**

3.14 **2020/21 plan progress:** JA explained that the plan was due to be approved by the ARC on 19 May 2020 but in the meantime, three of the top five reviews had been started: COVID-19 Assurance Programme, Maintain Minimum Control Standards and Cyber Security Maturity.

3.15 **Internal Audit reviews completed**: JA noted that the outcomes of the three final reviews:

- Postmaster on-boarding: This was rated as satisfactory and the new process was deemed effective with recommendations from GLO having been implemented.
- Vetting and Fit & Proper: This was rated as needs improvement due to the very fragmented processes that were in place and the lack of clear ownership. Fit & Proper was slightly better than vetting and improvement on vetting was expected when the ownership issues were resolved. It was explained that accountability had been split between the Operations team, HR and Compliance. It has been agreed to bring accountability into the Operations team within clear oversight from Compliance. The Fit & Proper policy was also being updated and LC was asked to ensure that HR were involved in this update. JH confirmed he had a new Vetting and Oversight Assurance Manager starting on 11 May 2020. **LC**
- Change Control Framework: This was rated as needs improvement. The Chair noted that he felt elements of the report were confusing and needed to be clearer. JA explained that this was a follow up review following a review last year which looked at gating, benefit realisation and second line assurance activity and outlined the need to establish a control framework for change activity.

POL00423570

The purpose of the present review had been to assess to what extent the previous recommendations had been implemented. It was noted that most findings had arisen from the self-assessment process (the Strategic Portfolio Office (SPO) had been quite conservative in its ratings) and that 29 out of 37 controls were assessed as partly effective. This sounded more serious that it was because this rating had been given if only one programme in the test had failed. JA was asked to ensure this context was clearer in the report. **JA**

3.16 **Status of Audit Actions**: JA noted that five actions were due at the end of April which had been harder to close due to other priorities relating to COVID-19. Some actions may need to be extended but any extensions would be agreed prior to the ARC on 19 May 2020. AG requested that JA send him any outstanding actions relating to the Commercial Team. **To do: JA**

3.17 Subject to the amendments as outlined, the Combined Risk, Compliance and Audit Update was **NOTED for onward submission to the ARC**.

4. Internal Audit Plan

4.1 JA explained that audit plans had become dynamic against moving targets due to the COVID-19 crisis and that he has been webinars with other heads of audit. This has shown that the Post Office approach has been similar to other organisations and a key element was that there may need to be some compromise on the maintenance of controls during the COVID-19 crisis. The top five priorities were outlined as:

- COVID-19 Programme Assurance/Support;
- Maintain Minimum Control Standards;
- Cyber Security Maturity;
- Health & Safety response to COVID-19 crisis; and
- Effectiveness of Second Line during COVID-19.

4.2 The medium priority reviews were outlined as:

- GLO Operations Improvement Programme;
- Postmaster Reporting;
- BCP Post-crisis assessment;
- Branch Hub; and
- Stamp Stock (relating to inventory controls).

BF noted that it would be helpful to have an external view of Stamp Stock and it was agreed that BF and JA would pick this up. JA explained that his internal review would only take place after the external review into stamps and whether management had led to systemic agent losses. Similarly the review into the GLO Operations Improvement Programme would be done after the planned external GLO response review. It was noted that this was a case of timing and consideration as to whether an end-to-end external review was required as the Norton Rose review was simply a gap analysis. JA was asked to look at this in conjunction with BF and JT. Regarding the COVID-19 Assurance Programme, MB questioned whether this would extend to the scope of Project Neo and risk and JA explained that this was not presently included but that he would discuss with MB. JA further noted that he had issued an interim report to Caroline Scott on the review of phase 1 of the COVID-19 Programme. In response to a questions from AJ regarding Postmaster Reporting, JA confirmed that he would discuss the scope of the review with her and her team nearer to Q3. **JA/BF** **JA/BF/JT** **JA/MB**

4.3 The Internal Audit plan, including the internal audit priorities during the COVID-19 crisis, was **NOTED for onward submission to the ARC.**

5. PCI-DSS and Cyber Security Update

PCI-DSS Programme Update

5.1 **Ingencio CEO call**: JS explained that CEO to CEO dialogue between Ingencio and Post Office had been established as requested by the ARC and there was diarised meetings between the Global Vice President of Ingencio for retail and banking and Nick Read. Written reports from the calls were provided to JS. It was noted that Ingencio were not reporting any direct implications for their services owning to COVID-19 at present.

5.2 **Integrated Programme Plan:** It was expected that the programme would obtain Ingenico final banking software deliverables in early February 2021 and branch rollout would commence in late March 2021. Branch rollout would be completed in May 2021 and formal PCI-DSS accreditation would be achieved by June 2021. The team has also held a deep dive into the plan itself and work was ongoing to see if the delivery plan timeline could be improved further. The business case for £15.8m would be presented to the Investment Committee and Board in May.

POL00423570

5.3 **PED rollout programme:** JS noted that this programme was presently on pause due to the COVID-19 crisis and the present thinking was that this would recommence in July, subject to the Government announcement on lockdown expected on 10 May 2020.

5.4 **Santander:** JS noted that most other organisations were compliant but that there had been some delays with Santander. The Chair questioned whether Post Office would have any recourse if we could not be compliant due to them. JS explained that the target operating model included the ability to pay Santander credit cards and that this could be a point of leverage, but at present, we were not setting out to utilise this. The issues Santander were facing seemed genuine and Nick Read had already been on a series of calls to try to resolve.

5.5 The PCI-DSS Programme Update was **NOTED for onward submission to the ARC.**

Cyber Security

5.6 **Cyber Security Maturity**: TJ outlined that the maturity score was averaging 2.4 in mid-April and he hoped this would improve to 2.45. This figure was an estimate and it would be retested by Deloitte and Jonathan Acres from Post Office from 11 May 2020. This retest would allow the reassessment target maturity due to recent events. A new change programme was being developed to close any gaps identified and an update would be provided to the next RCC.

5.7 **COVID-19 risk, issues and threats:** The team has been working with Data Protection and IT Operations to enable people to work from home, but they were also ensuring that any exemptions to our usual policies were being closed down rapidly. Data loss was also being monitored, although a slightly softer approach was being taken to enable home working. Work had also been completed to ensure the IT Service desk can communicate with colleagues securely. It was noted that the team was feeding into and monitoring the National Cyber Security Centre's (NCSC) work on COVID-19 threats. The mains threats were fake Post Office websites and phishing. During the COVID-19 crisis, security threat activity was up between 25% and 55% depending on the type of activity which included money miles and password attacks.

5.8 **Social media presence**: TJ outlined that in response to the RCC action the guidance on protecting ourselves on social media had been shared with the Board and GE. Links to the guidance were available in the paper.

5.9 The Chair requested that a more extensive update on the Joiners/movers/leavers programme was included in the paper for the ARC on 19 May 2020 and that a draft should be reviewed by the Chair. **TJ**

Subject to the amendment as outlined, the Cyber Security Update was **NOTED for onward submission to the ARC.**

6. Progress Update on the Pilot Implementation of the Contract Management Framework

6.1 BF explained that 142 top material contracts had been identified. By the end of the pilot (19 May 2020), it was expected that 60 material contracts would have been uploaded to Web3.0 having had their obligations mapped at a cost of £100,000. The balance of 82 material contracts would take a further month to upload at an additional cost of £26,000. There were also 1,500 other contracts which have not been uploaded to Web3.0 and had their obligations mapped. It was recommended that due to the current commercial environment, the pilot should work to complete the upload and mapping of obligations for the top 142 material contracts but that the other contracts should not be uploaded as part of the pilot and should be uploaded during the natural contract lifecycle (as amendments or extensions arise). It was proposed that the accredited external training which had been budgeted for at a cost of £80,000 was not pursued, releasing this money back to the business and for £26,000 to be reallocated to support the mapping of the outstanding material contracts. The Chair requested that BF discuss the approach with Carla Stent, ARC Chair, prior to submitting the paper to the ARC to get a steer as to whether this approach would be acceptable. **BF**

The RCC NOTED the paper and APPROVED the following for onward submission to the ARC, subject to BF gaining steer from the ARC Chair as to whether this approach was acceptable:

- While internal training has been provided, accredited external training will not be provided to identified contract managers for material contracts, accepting the risk that this may result in a baseline level of capability not being established amongst this group of individuals.
- Reallocating £26,000 of the £80,000 originally included in the budget to provide external training in order to complete the upload and mapping of all remaining contracts identified by GE as being material in terms of strategic and financial value by the end of June 2020 ("Material Contracts").
- It is proposed that the implementation of CMF across those contracts not identified as being material by the GE ("Other Contracts") be done outside of this project through the natural 'lifecycle of a contract' e.g. as they are renewed, cease or new agreements are entered into. This will take significantly longer, through BAU resource and processes, but release c£700k from the 20/21 Change Portfolio Budget.

POL00423570

7. Horizon Scanning Update

7.1 BF explained that this was a new report for the RCC and had been presented to assist in the enhance of the legal maturity of Post Office by ensuring that the Board and Executive team were proactively managing legal and regulatory risks as they develop. This was supplemented by regular Law In Trends forums which were cross-functional and looked a legal and regulatory changes on the horizon and discussed how Post Office might need to respond. The Chair complimented the paper and BF confirmed that the paper would be developed over time to include a Red/Amber/Green (RAG) status against each element.
The Horizon Scanning Update was **NOTED for onward submission to the ARC.**

8. Supplier Contract out of Governance

8.1 BB explained that there were no contracts out of Governance that required approval as all approvals had been addressed at the Board on 8 April 2020. The Chair requested that the paper be reorganised to cover new requests first, then any future contracts on the horizon and then any past approvals. **BB**

8.2 On the future contracts that were high value and at risk of being awarded or extended non-compliantly, BB outlined the following:

- End User Computer services (EUC) (value of £10m): Discussions were still being held between IT and the Change project team as to whether there would be sufficient funding to run a procurement. A paper regarding this project was being prepared for the GE on 13 May 2020.
- Common Digital Platform (CPD) (value of £5m): There was an option for a six month extension to December 2020 on a short term basis to allow for cloud migration and long term strategy adoption. This was already being discussed with the supplier to enable an extension whilst a procurement process is run.
- Brands/Rapp (value of £1.3m): The sourcing process has not been agreed with the business and their appetite to migrate the service was limited. Funding was also an issue.
- ATM support (value £350,000): There were a number of contracts expiring in August 2020 which may need to be extended non-compliantly whilst the tender process continued.
- Identity Services (value of £5m): A full sourcing plan has been agreed to be funded out of OPEX Identity budget, but this has been derailed by the COVID-19 crisis. Discussions were ongoing between Martin Edwards, Digidentity and Legal to ensure extension to March 2021 which would give more latitude to manage the OJEU required and would give the business more time to review other options. In the interim, discussions were ongoing with the Commercial team as to whether our approach needed to be changed given COVID-19 crisis.

It was further noted that otherwise the procurement pipeline was very quiet. This was thought be to because feedback had gone to the business explaining that risks would not be excepted and because of the spending freeze.

8.3 Subject to the outlined amendments, the Supplier Contracts out of Governance Update was **NOTED for onward submission to the ARC.**

9. Cooperation with Law Enforcement Agencies and Addressing Suspected Criminal Misconduct Policy

9.1 BF explained that this was a policy to cover how Post Office dealt with suspected criminal misconduct covering private prosecutions and cooperation with third party law enforcement agencies, regulators and industry accredited bodies. The policy sought to balance the following risks: safeguarding the integrity of HNG-A so that it is not unnecessarily undermined or brought into question without the proper governance around the release of information against being seen to support and cooperate with law enforcement agencies. The approach would be that we would support third parties to investigate criminal misconduct if there were mandatory requirements. Where it was not mandatory, we could exercise discretion as to whether to assist but it was a question of who within the business would have the authority to authorise the release of information. We have taken risk based approach: where the data would not rely solely on integrity of the Horizon system (i.e. other evidence such as CCTV existed), and therefore the integrity of HNG-A was unlikely to be brought into question, we would provide the data to the requesting body. BF further outlined that there was a risk with the policy in that it could not prevent potential law enforcement proceedings if they struck at the heart of the Horizon system and this could mean that the integrity of the current Horizon system was called into question. Therefore work still needed to be done with IT to be able to substantiate that there were no known bugs and this needed to become a BAU process.

9.2 BF noted that the team would undertake an "optical review" of the policy before it was presented to the ARC. This was because, although such documents would not usually be discoverable, it could do so in the future. As such the policy needed to be reviewed to consider how it may be viewed by the public. BF further outlined that the policy would prohibit Post Office from engaging in private prosecutions without the

POL00423570

express consent of the Board. It was also noted that any data provided from legacy or HNG-X Horizon would be provided with a health warning given the findings of the Horizon judgment.

9.3 JS cautioned that there would be a cost to operationalise this policy as a process would need to be in place to deal with any approaches from law enforcement agencies, regulators or registered industry bodies. We needed to ensure that we had the skills, capacity and money to deliver. BF explained that the policy included a process map but that he would highlight this at GE to ensure that the consequences of the policy were understood. **BF**

9.4 It was further noted that requests for data may not be easy to fulfil if it required cooperation from third parties including Fujitsu and Ingenico. JS explained that it needed to be recognised that this involved some very comprehensive relationships. BF concurred but noted that this would be mitigated by general law cooperation clauses within contracts. AG noted that the paper was very "Horizon-specific" but that the policy had a much broader systems reach. BF explained that the policy was designed to cover all requests, but that HNG-A was an area of particular sensitivity. It would be supported by a cross-functional team including compliance and IT security. As such, support would be provided to the business. JT suggested that a list should be compiled of colleagues who could provide information to law enforcement agencies, regulators and industry bodies to ensure compliance.

9.5 The Criminal Misconduct and Cooperation with Law Enforcement Agencies paper and attached draft policy entitled "Cooperation with Law Enforcement Agencies and Addressing Suspected Criminal Misconduct" was **APPROVED for onward submission to the ARC**. In approving the draft policy, the RCC also:

- decided that Post Office's policy should be to cooperate with mandatory requirements and voluntary requests by law enforcement agencies where the risk to undermining the integrity of HNGA is low or low/medium;
- approved, with respect to the Tools supporting the Policy:
  a. the process for determining what information can be provided to law enforcement agencies for intelligence purposes (Tool 1);
  b. the process for determining when evidence can be provided to law enforcement agencies (Tool 2); and
  c. the process for proactively disclosing to law enforcement agencies disclosable material in criminal cases where Horizon-derived data is being used (Tool 4);
- decided that Post Office's policy should be not to conduct any private prosecutions at present; and
- decided that Post Office should report internal criminal misconduct to the police and ask Post Office operators to advise Post Office if they make a victim crime report.

10. Review of draft Audit, Risk and Compliance Committee meeting agenda for 19 May 2020

The draft ARC agenda for 19 March was **NOTED** and RW was requested to confirm with Carla Stent (ARC Chair) and JS the scope of the "broader Fujitsu update" and to add a noting paper for the Supplier Contracts out of Governance update. **To do: RW**

11. Any other Business

There was no other business.

DRAFT

POL00423570

Post Office Limited Risk and Compliance Committee Actions
Updated: 09.07.2020

REFERENCE	ACTION	ACTION OWNER	DUE DATE	STATUS	OPEN/CLOSED
		RCC Meeting 06.05.20			
3.3 Combined Risk, Compliance and Audit Update: Risk	**Risk**: COVID-19 wider enterprise risk statement be considered at the GE in June 2020 (MB to request a GE agenda slot with Veronica Branton, Company Secretary).	MB	June 2020 – *please provide exact date*	On the GE Tactical agenda for 26th June 2020.	Open
3.9 Combined Risk, Compliance and Audit Update: Compliance	**Belfast Data Centre Exist and move to the Cloud**: The Chair questioned who was having the client conversations and it was highlighted that there should be engagement with client management owners. JH was asked to pick this up with the Commercial team and JS was asked to check with the IT Project Team.	JH/JS	*Please provide suggested due date*		Open
3.10 Combined Risk, Compliance and Audit Update: Compliance	**Whistleblowing**: The Chair asked that he was provided with information as to the kind of issues that were being raised by whistle blowers	JH	*Please provide suggested due date*	Update 09/07/2020**:** a list of whistleblowing types/issues has been provided in the whistleblowing report to be presented at RCC 13/07/2020.	**Recommended for Closure**
3.10 Combined Risk, Compliance and Audit Update: Compliance	**Whistleblowing**: The Chair requested that the investigations were reviewed on a case-by-case basis with HR and challenge the assumption that the investigation had to be paused. If a major issue was subject to the complaint, the response needed to be balanced.	JH	*Please provide suggested due date*		Open
3.11 Combined Risk, Compliance and Audit Update: Compliance	**External Threats – Lottery:** The wording of the section would be reviewed before submission to the Audit, Risk and Compliance Committee (ARC) so that it was clearer.	JH	19/05/2020 (ARC Meeting)	The wording of this section was revised for the ARC paper as submitted for 19/05/2020.	**Recommended for Closure**
3.12 Combined Risk, Compliance and Audit Update: Compliance	**Dangerous Goods**: A project had been initiated to place the onus on the customer to confirm what was in their parcel via a validation on the Pin Pad (to reflect the SSK process). The Chair requested that this section of the paper be updated prior to submission to the ARC to better outline this project.	JH/AJ	19/05/2020 (ARC Meeting)	The wording of this section was revised for the ARC paper as submitted for 19/05/2020.	**Recommended for Closure**
3.13 Combined Risk, Compliance and Audit Update: Internal Audit	**2019/20 plan progress**: AG was asked to chase the Commercial Team to ensure that management comment was provided as soon as possible to enable the	AG	19/05/2020 (ARC meeting)	This action was completed by Chrysanthy Pispinis on 06/05/2020.	**Recommended for Closure**

POL00423570

Post Office Limited Risk and Compliance Committee Actions
Updated: 08.07.2020

	complete reports to be ready for the ARC on 19 May 2020.				
3.15 Combined Risk, Compliance and Audit Update: Internal Audit	**Internal Audit reviews completed**: The Fit & Proper policy was also being updated and LC was asked to ensure that HR were involved in this update	LC	*Please provide suggested due date*	LC has spoken to JT and an update will be provided in September.	Open
3.15 Combined Risk, Compliance and Audit Update: Internal Audit	**Internal Audit reviews completed**: It was noted that most findings had arisen from the self-assessment process (the Strategic Portfolio Office (SPO) had been quite conservative in its ratings) and that 29 out of 29 controls were assessed as partly effective. This sounded more serious that it was because this rating had been given if only one programme in the test had failed. JA was asked to ensure this context was clearer in the report.	JA	*Please provide suggested due date*	The report wording has been updated and the report was re-issued ahead of the ARC.	**Recommended for Closure**
3.16 Combined Risk, Compliance and Audit Update: Internal Audit	**Status of Audit Actions**: JA noted that five actions were due at the end of April which had been harder to close due to other priorities relating to COVID-19. Some actions may need to be extended but any extensions would be agreed prior to the ARC on 19 May 2020. AG requested that JA send him any outstanding actions relating to the Commercial Team.	JA	*Please provide suggested due date*	A list of actions related to Commercial was sent to AG. Extension was given for 14 actions which were delayed due to COVID-19. This was reported to the ARC and the actions continue to be tracked.	Open
4.2 Internal Audit Plan	**Stamp Stock**: BF noted that it would be helpful to have an external view of Stamp Stock and it was agreed that BF and JA would pick this up. JA explained that his internal review would only take place after the external review into stamps and whether management had led to systemic agent losses.	JA/BF		Completed – KPMG are conducting a review of this area at the moment. Internal audit is considering scope of potential future audit. 13/7/20 **This was discussed. A review is currently being performed by an external firm. Stamp Stock remains on the IA plan for Q4.**	**Recommended for Closure**
4.2 Internal Audit Plan	**GLO Operations Improvement Programme**: The review into the GLO Operations Improvement Programme would be done after the planned external GLO response review. It was noted that this was a case of timing and consideration as to whether an end-to-end external review was required as the Norton Rose review was simply a gap analysis. JA was asked to look at this in conjunction with BF and JT.	JA/BF/JT		Completed – NRF are continuing their work. An external comprehensive audit will be completed around Q2/3 to confirm/provide assurance on the remediation of any gap analysis conducted as a result of the NRG work. 13/7/20 Agreed with JT to delay the audit to Oct 2020 and limit the initial scope to recommendations from the Common Issues Judgement.	**Recommended for Closure**

POL00423570

Post Office Limited Risk and Compliance Committee Actions
Updated: 08.07.2020

4.2 Internal Audit Plan	**COVID-19 Assurance Programme**: Regarding the COVID-19 Assurance Programme, MB questioned whether this would extend to the scope of Project Neo and risk and JA explained that this was not presently included but that he would discuss with MB.	JA/MB	*Please provide suggested due date*	The review of the COVID-19 Programme assessed the extent to which actions were transferred to NEO. Project NEO has been added to the IA plan.	**Recommended for Closure**
5.9 PCI-DSS and Cyber Security Update	**Joiners/Movers/Leavers**: The Chair requested that a more extensive update on the Joiners/movers/leavers programme was included in the paper for the ARC on 19 May 2020 and that a draft should be reviewed by the Chair.	TJ	19/05/2020 (ARC meeting)	Update 08/07/2020: paper to be presented at RCC (13/07/20) and ARC (27/07/2020). This was included in the paper and sent to the chair ahead of the ARC. Subsequent papers will include regular updates.	**Recommended for Closure**
6.1 Progress Update on the Pilot Implementation of the Contract Management Framework	The Chair requested that BF discuss the approach with Carla Stent, ARC Chair, prior to submitting the paper to the ARC to get a steer as to whether this approach would be acceptable.	BF	Prior to 19/05/2020	BF had this conversation and the ARC Chair was supportive of the approach. Paper prepared and to be presented at the March ARC.	**Recommended for Closure**
8.1 Supplier Contract out of Governance	The Chair requested that the paper be reorganised to cover new requests first, then any future contracts on the horizon and then any past approvals.	BB	19/05/2020 (ARC meeting)	Paper was amended accordingly and presented to the ARC.	**Recommended for Closure**
9.3 Cooperation with Law Enforcement Agencies and Addressing Suspected Criminal Misconduct Policy	BF explained that the policy included a process map but that he would highlight this at GE to ensure that the consequences of the policy were understood.	BF		A process map is included in the policy.	**Recommended for Closure**
RCC Meeting 14.03.20					
3.3 - Cyber Security	Internal audit would be commissioned to complete an audit on FRES (subject to approval in the master services agreement).	BF	13/07/2020	Sherrill Taggart has asked the Legal Team to review the FRES contract. Will be completed before the next RCC. Update 18/05/2020: This was completed and update was provided to JA & JH. In summary the FRES JVA does contain an audit right for a shareholder but not a unilateral one. Therefore we would need BOI's consent to carry one out.	**Recommended for Closure**
6.6 Annual Legal Risk Report 2019/20	The Committee questioned whether these examples had been flagged to the Committee or ARC before? [Post meeting note – these issues have not been raised previously to the Committee or to ARC.]	DP/RW	~~06/05/2020~~ 13/07/2020 (RCC Meeting)	These issues have not been raised previously to the Committee or to ARC. Update 06/05/2020: The issues being flagged to the RCC or ARC was questioned as to its context. It was requested that more information was	Open

POL00423570

Post Office Limited Risk and Compliance Committee Actions
Updated: 08.07.2020

				provided as it was not enough to simply say that it was not raised. Update 21/05/2020: Context: This action was in respect of Competition Law and the acquisition of PZBPL – *"Following the acquisition of Payzone Bill Payments Limited (PZBPL) , the legal team has provided advice/guidance on sharing commercially sensitive information between POL and PZBPL, conflicts of interest, and going to market service offerings. Examples of issues have included PZBPL management (POL staff members) seeking to make decisions on behalf of POL rather than PZBPL and requests from PZBPL for confidential information held by POL in breach of confidentiality obligations to a mutual client. "*	
RCC Meeting 14.01.20					
10.6 - Money Laundering Reporting Officer (MLRO) Annual Report	BF, SS and JH talk to retail on enforcing three lines of defence and suggested BF attend a meeting with HMRC.	SS/JH	*Please provide suggested due date*	09/07/2020: HMRC are not conducting meetings at present due to Covid, but Sally has chased. Delayed due to scheduled meetings being postponed. Update from Sally: We have been unable to arrange the meeting with Ben and HMRC as yet – our new Supervisor was appointed end February, but since Covid-19 lockdown, HMRC are not undertaking any Compliance activity, and clearly we are not able to meet. If the current situation continues, I will see if we are able to sort out a meeting for Ben via Teams.	Open
RCC Meeting 07.11.19					
3.2 Supplier Contracts out of Governance	SSK – retail lead team decision required to ensure project does not stall.	Kathryn Sherratt/ Nick Wade /CM/Marketing	*Please provide suggested due date*	In progress – subject to PSG funding. 'On hold' given the change re-prioritisation. OJEU process is being finalized to demonstrate progress since action was set. The SSK Procurement Project is on hold at present. This work will now form part	Open

POL00423570

Post Office Limited Risk and Compliance Committee Actions
Updated: 08.07.2020

				of NEO Work Package 5, which is due to report to Board in June and July on Network Shape and Formats and Propositions respectively. NEO WP5 will return to Board in September with the Technology part of the work stream, the direction from which will form part of the Procurement. The project will return to PRB to resume work following the September Board.	
3.3 Supplier Contracts out of Governance	Brands/RAPP – Agree date for tender	~~SH~~ JS / Marketing	*Please provide suggested due date*	In progress – subject to PSG funding.	Open
5.3 Cyber Security	A major incident test be completed with findings reported to the Committee.	TJ/JS	~~January 2020~~ 13/07/2020 (RCC Meeting)	The test was scheduled for March but was interrupted by preparations for COVID – to be rescheduled. Update to be provided in Cyber Security update paper. Update 06/05/2020: JS to provide an update.	Open
5.3 Cyber Security	Joiners/movers/leavers – to review whether contractors who no longer work for POL have been removed from POL emails and systems.	DZ/LC/TJ	~~January 2020~~ 13/07/2020 (RCC Meeting)	Update 08/07/2020: a paper is being presented at RCC and ARC (13/7/20 and 27/7/20 respectively). Review is complete and all that no longer work for Post Office were removed as of 31 December – ongoing checks and MIM project will help to ensure that there are no further orphaned contractors in the system. A paper is to be presented to GE. Update 06/05/2020: TJ to provide an update.	**Recommended for closure**

POL00423570

3

POST OFFICE LIMITED RISK AND COMPLIANCE COMMITTEE REPORT

Title:	Risk, Compliance and Audit Report	**Meeting Date:**	13 July 2020
Author:	Mark Baldock: Head of Risk Jonathan Hill: Director, Compliance Johann Appel: Head of Internal Audit	**Sponsor:**	Al Cameron: Chief Financial Officer Ben Foat: General Counsel

Input Sought: Noting

Previous Governance Oversight: Not applicable

Executive Summary

This paper provides an update on key and emerging risks, compliance matters and an update on the latest internal audit position. The Committee is asked to:

1. Note the Risk update, specifically:
   - the status of the Post Office's risk data set and the key risks
   - the Post Office's approach to risk appetite and Key Risk Indicators
   - how the Post Office is embedding accountability and responsibility for the management of its risks
   - the new Risk Lead role
   - the status of the Change Portfolio and key delivery challenges.

2. Note the Compliance update.

3. Note the Internal Audit update, specifically:
   - analysis of internal control themes from 2019/20
   - audit report clearance metrics
   - progress being made with delivery of the Internal Audit programme and completion of audit actions.

Confidential

POL00423570

3

Risk

Questions addressed

1. What is the status of the Post Office's risk data set and what are the key risks?
2. What is the Post Office's approach to risk appetite and Key Risk Indicators?
3. How is the Post Office embedding accountability and responsibility for the management of its risks?
4. What is the new Risk Lead role?
5. What is the status of the Change Portfolio and key delivery challenges?

The Post Office's risk data set & the key risks

1 In 2/2020 we (in Central Risk) facilitated a discussion with GE to discuss the key business risks faced by the Post Office and their (then) current RAG status and relative priority. Following that discussion we have now completed work on the articulation of a new Post Office-wide three-tiered risk data set comprising (i) **15** overarching enterprise risks, (ii) **70** linked intermediate risks and (iii) **350** subsidiary local risks. All **435** of these have been uploaded onto RSA Archer (our corporate Governance, Risk and Compliance tool) and arrangements are underway for these risks to now be proactively managed by the business. This work is ongoing but includes **ensuring the business clearly articulate each risk**, (in terms of its cause, the risk itself and its impact), **'grouping' low level risks** to their relevant intermediate and enterprise risks (to give an aggregate risk profile), **assessing risk impact and likelihood consistently** (against corporate standards) and, finally, **outlining clear remediation plans** (with owners and dates).

2 At this point the key enterprise risks remain:

- Commercial: Risk the Post Office Commercial proposition is unattractive because the existing products are too complex or confusing, new product are cost ineffective, unable to be scaled and unattractive to the market
- COVID-19: Risk that the Post Office business employees/postmasters are adversely impacted by the spread of COVID-19 and wider associated socio-economic activity.
- Financial: Risk that the Post Office has insufficient funding and/or uncontrolled costs in the short-, medium and long-term such it is unable to deliver its strategic objectives. This could have a long term impact on commercial viability
- Legal: Risk that the Post Office is unable to comply with legislative and regulatory changes, sectoral regulator guidance and/or the outcome of other external legal activity (i.e. litigation) resulting in significant fines, loss in revenue, reputational damage and customer detriment
- Technology: Because the Post Office is heavily reliant on key 3rd IT parties (with limited ability to influence the relationship), has an ageing IT infrastructure, hardware and software there is a risk that it is unable to deliver a new Front Office system and has an ineffective Disaster Recovery regime. If the risk is not proactively treated and materialises this could lead to significant impact to operations and significant reputational damage.
- Operational: Because of low-quality Branch Network locations, unprofitable Retail Partner(s), an unattractive Agency remuneration package and/or badly designed operational core processes & control environment there is a risk that the Post Office operation is not fit for purpose.

3 Key intermediate risks include:

- Government Services: The Post Office's revenue from the provision of Government Services (i.e. Digital Check & Send, IDPs) may reduce over the short-, medium-

Confidential

POL00423570

and long-term. Work is underway to review a faster roll out of Tablet services to ensure we are ready for the travel bounce-back. Marketing discussions underway for a PO services awareness campaign. Regular liaison with Government Departments to emphasise role PO can play.

- Digital Income: Post Office on-line products and services may generate a reduced income level compared to comparable physical products and services. Commercial work underway to determine post-COVID-19 strategy and identify critical markets for Post Office along with the requisite operational functions and dependencies to support them.

4 Since the last ARC we have fully assimilated the Post Office COVID-19 risk identification and management activity into our wider enterprise risk work given ongoing separation would have been simply artificial.

5 Appendix 1 provides a series of Dashboards (at enterprise, intermediate and risk register level). The data is taken directly from RSA Archer.

Risk Appetite & Key Risk Indicators

6 Each risk within the Post Office risk data set is assessed for impact and likelihood against the corporate scoring metric (the Post Office HARM table approved by ARC in 9/2020). This assessment provides each risk with (i) an **inherent score** (before any mitigation is undertaken), (ii) a **residual score** (reflecting the impact of mitigations to date) and a **target score** (an aspirational end point when the business consider the risk can be simply tolerated).

7 However for these assessments to be of any value we must be able to differentiate between individual risks with identical impact and likelihood scores. Without this the assessments will simply be too 'crude'. To do this we need different tolerances at a corporate level for different types of risk. We also need a simple early warning system to show us where such tolerability is under strain.

8 Given this we have secured GE approval to our proposal to refresh our corporate risk appetite statements (last updated in 2015) and put in place a supporting set of Key Risk Indicators (KRIs). Such approval was on the basis that we

- minimise the bureaucracy and burden on the business and use existing performance data to help shape the associated KRIs;
- ensure the risk appetite statements cover cross-organisational risks, not just those in organisational silos; and,
- pilot the approach in 3 areas (i) **Operational/Legal** (ensuring we cover Postmasters/GLO etc), (ii) **IT** (ensuring we cover Technology, Security and extended IT supply chain risks) and (iii) **Finance**.

9 We have already begun work on the Operational/Legal and IT risk appetites. This involves

a) an initial desk-based review by Central Risk and the completion of a simple questionnaire on the topic by key individuals within the business to identify initial options

b) a Central Risk-facilitated discussion with the GE members and their senior management team to re-confirm the key risks they face, their associated KPIs and what should be the likely tolerances and acceptable trade-offs to allow them to remain within an agreed level of appetite

POL00423570

c) the completion by Central Risk and the GE Risk Lead of the final draft Risk Appetite Statement and KRIs for GE sign-off and then submission to RCC/ARC.

10 We intend to seek RCC/ARC approval to the final draft outputs from 9/2020. At approval we will produce supporting communications and guidance for the business on how agreed Risk Appetite Statements and KRIs will be governed and can be used pragmatically and sensibly going forwards. We plan for approved risk appetite statements to be subject to yearly review thereafter.

Accountability and Responsibility for management of risk

11 Since the last ARC we have also clarified where accountability and responsibility should lie in the business for managing and owning our risks. The GE has re-confirmed its commitment to the industry standard "three lines of defence" risk management model. It is a simple and effective way to delegate and coordinate risk management roles and responsibilities. We have clearly communicated that for the Post Office this means:

- 1st line of defence: The GE Commands (and their individual directorates/units) are the Post Office's 1st line. They own and are accountable for identifying, assessing managing and reporting on their risks. They are also responsible for putting in place internal controls on a day to day basis, ensuring compliance with risk policy and implementing corrective actions to address any deficiencies.
- 2nd line of defence: We, in Central Risk are the Post Office's 2nd Line. We define and implement the Post Office's risk standards, policies, procedures and guidance. We also proactively support and guide the GE Commands in the management of their risks in line with good practice. We alert senior management to emerging issues and changing risk scenarios. We also monitor and report on levels of compliance (including agreeing exceptions to approved risk policies). We report to the GE, RCC and ARC on the Post Office's current and emerging risks profile.
- 3rd line of defence: Internal Audit remain the Post Office's 3rd line. They provide an objective and independent evaluation of how effectively the Post Office assesses and manages our risks, including the operation of the 1st and 2nd lines.

Risk Leads

12 To ensure this model works effectively the GE have nominated Risk Leads to proactively coordinate and support the risk work within their respective GE Commands.

13 The Risk Lead is an important role. As such the individuals appointed have the requisite authority to help and direct their respective individual directorates/units in identifying, assessing and managing their risks. They will act as role models for Post Office risk management in their GE Group.

14 We, in Central Risk, are proactively supporting them in this role through informal training, guidance etc as well as facilitating risk workshops etc. We will also soon be arranging for them (and individual risk owners) to be given direct access to the RSA Archer risk management software tool. This will allow them to access and manage their risks efficiently and effectively on-line and in real-time.

The status of the Change Portfolio, including top risks and key delivery challenges

15 By the end of 5/2020 the overall status of the Portfolio remains at Amber. The detailed review of the Change Portfolio, as a result of changing costs and COVID-19 has

POL00423570

continued with a baseline position and options for prioritisation discussed at the Board in May. Prioritisation will continue while under extreme conditions.

16 YTD spend by the end of 5/2020 was £6.5m. This was lower than expected due to delays in approvals for litigation spend. YTD benefits achieved were £5.2m which was £1.2m below forecast, driven mainly by product related variances

17 Delivery remains amber with a lot of activity around project closures, 4 projects closed in 5/2020 and 9 are planned close by the end of 8/2020. People and Culture programmes are due to commence in the future months.

18 The number of gold and platinum projects reporting an overall Red RAG status is **4**. This is unchanged since the last RCC/ARC but the individual projects are different:

- IDS Digital Identity: In 4/2020 the Portfolio Review Board approved for the IDS In Branch Verification workstream to be de-scoped from this project and established in its own right. This allows the IDS Digital Identity project to proceed to early closure.
- Paystation Refresh: Despite an excellent start to rollout (10% of Paystations having been refreshed to date) overall, status remains Red because of the impact of COVID-19 on rollout. This inhibits our ability to deliver the British Gas contractual requirement for additional transactional data by 1 August 2020.
- General Data Protection Regulation (GDPR): Overall Red status because there are a small number of contracts in which the counterparties are not engaging. Plan to continue remediation in BAU.
- Post GLO (Legal): Level of risk is unquantifiable due to the potential for a high number of referrals to the Court of Appeal which could lead to a high number of overturned convictions

19 Appendix 2 provides a summary of the current key 'Platinum and Gold' change programmes and their current reporting status.

Compliance

Telecoms

Telecoms provider response to Coronavirus

20 The call centre is stable and has resumed normal activities, with 85% of agents homeworking as of 23rd June. Post Office is continuing to prioritise fault repairs for vulnerable customers and honour the commitments made to DCMS. Ofcom are continuing to request weekly updates and have now resumed their monitoring and enforcement programme.

Fairness

21 Fairness for customers is a priority for Ofcom and they have a significant work plan to help achieve this. Post Office along with all the other major providers signed up to Ofcom's fairness commitments earlier this year which are to ensure:

- Customers get a fair deal, which is right for their needs.
- Customers get the support they need when their circumstances make them vulnerable.
- Customers are supported to make well-informed decisions with clear information about their options before, during, and at the end of their contract.

POL00423570

- Customers' services work as promised, reliably over time.
- Customers can sign up to, change and leave their services quickly and smoothly.
- Customers can be confident that fair treatment is a central part of their provider's culture.

22 Ofcom will be collecting data over the next few months with a view to publish a report on the fairness commitments in early 2021. At our last meeting with Ofcom they said that they consider customers as "vulnerable" when they have been out of contract for a long time e.g. 2-3 years. Ofcom thought Post Office would be near the top of providers with a high percentage of out of contract customers (paying higher prices than in contract customers). Ofcom said they would 'like progress' on long term out of contract customers. Some providers had already taken steps to address this, e.g.

- BT has provided a one-off automatic price reduction for vulnerable customers who are already out-of-contract.
- TalkTalk has agreed to carry out an annual review to ensure that its vulnerable customers who are out-of-contract are placed on the best tariff
- Virgin Media is calling vulnerable customers (including anyone over 65) to get them onto the best contract and, if they do not answer, will automatically move them onto the best available price.

23 Budget constraints currently inhibit Post Office from acting in a similar fashion to other providers. It should be noted though that POL have implemented the End of Contract Notification Regulation which is driving customers to contact POL to renew their offer and is achieving good response rates.

Annual Best Tariff Notifications

24 Following on from the introduction of End of Contract Notifications, Post Office is required to send Annual Best Tariff Notifications (ABT) to customers who have been out of contract for more than a year and not received an End of Contract Notification. The ABT must be sent by 14th Feb 2021. The telecoms team are aiming to do a trial to assess the impact ABT will have on the call centre so that we can resource effectively. Following on from this the telecoms team hope to do a phased approach starting with vulnerable customers.

25 This is subject to internal funding sign off. Final costings for delivery across this and other projects by Fujitsu is coming in higher than budget which is causing the telecoms team to have to review their plans for their year to complete the programme in line with the £1.2m initially approved budget.

PSD2

26 In January 2020 Post Office wrote to the FCA to inform it of our intention to seek an Electronic Communications Exemption ("ECE"). This requires Post Office to cap premium rate calls at £40 per call and £240 per month in aggregate. We informed the FCA that we would repay any over charged customers going back to when the obligations came into effect on 13th January 2018. The FCA confirmed it was happy with our approach. We wrote back to the FCA on 10 June 2020 to update them on the work we have been doing.

27 The FCA responded on 29th June 2020 to thank us for our clear letter and confirm they are happy with the approach we set out. Our next steps will be to:

- submit a first ECE Notification as soon as practicable (the FCA have not given us a hard and fast deadline as they say that most of the works appears to have been done already)
- submit an audit opinion in 2021 (date to be determined)

POL00423570

Emergency Database Update

28 Telecoms providers have an obligation to provide the address of a customer to the emergency services when a customer calls them. BT holds an emergency address database and it is common in the industry for mismatches to occur between a provider's address and the address stored in the system for billing purposes. This is because for example, a house gets made into flats, or a postcode gets change.

29 In order to mitigate this Talk Talk has a process in place whereby it checks the addresses on file against the emergency database. When it identifies mismatches it is usually able to correct these. However, in March 2019 Talk Talk informed Fujitsu, who in turn informed Post Office, that there were 568 cases it was unable to reconcile. Post Office began the process of resolving the mismatch and 79% of customers have confirmed their addresses. In the majority of cases it was the emergency database that was incorrect. Of the remaining customers, these have received a letter and received at least 3 outbound calls (both to landline and mobile where applicable) but have not responded so have now had their services limited in order to force them to contact Post Office and confirm their address.

30 Currently 99.9% of the addresses on the Post Office system match the emergency database. A new process has been set up so that every month Talk Talk provide any mismatches they cannot resolve and Post Office handle these through a BAU process.

European Electronic Communications Code

31 The new European Electronic Communications Code (EECC) will impose new regulatory obligations on all providers. These obligations will include changes to the switching process, additional information about contracts, provision of pre-contract information and accessibility obligations.

32 Ofcom recognise that given the very challenging circumstances we are currently in as a result of the coronavirus crisis, providers need additional time to make the necessary changes. Ofcom have said they are now giving providers at least 12 months from the date of the publication of their statement to implement these new rules, with the statement expected to be published in September however these rules were initially due to be implemented by December 2020.

33 Given the magnitude of the changes, Compliance and the Telecoms Team are commencing work now to understand how long the changes will take and the costs involved.

Responses to Ofcom information requests

34 In the March paper we noted that we have identified a number of inaccuracies in previous responses to Ofcom's formal S136 and S137 information requests for Comparing Service Quality. Fujitsu is continuing to work on the fix to the reporting but a plan is in place and we expect to get the corrected data by the end of June.

35 Ofcom were made aware of this issue when it was discovered. We were due to send the next round of data in July but Ofcom have now requested 12 month data instalments from all Communication Providers which means the next submission is January 2021.

36 Failing to provide accurate and timely responses to requests can result in an investigation by Ofcom's enforcement team and could result in fines.

Data Protection

GLO and Historic Shortfall Scheme

POL00423570

37 Compliance has been working with the GLO project to identify, locate and provide all data required to support the various ongoing initiatives, in particular;

- Working with the Historic Shortfall Scheme to manage and answer all requests for information and data to support applications. As of 24.06.2020 there are currently 55 live requests.
- There are another c.130 applications that will require additional data to support but we have yet to have requests made to us. These applications gaps range from information about any shortfalls suffered during their tenure through to full complex Data Subject Access Requests that could take up to 3 months to complete. We are proposing to the HSS team that Post Office should contact these applicants offering assistance.
- Provide information to support those cases that have been referred by the CCRC. These searches are complex and Compliance is working with external law firms to identify, locate and extrapolate all information that may be required by the Court.

38 Given the scale and complexity of these searches, the historic nature of the information and the widespread location of the data this has stretched BAU resources. The GLO SteerCo has approved additional resource to support this work.

39 In addition to this direct work, indirectly the Data Protection team is dealing with an unprecedented rise in complex Freedom of Information Requests relating to GLO matters. These requests invariably require external legal support due to their sensitivity and complexity. All requests prior to any disclosure require approval from the GLO Steerco and notification to UKGI.

GDPR Contract Remediation:

40 Please see separate agenda item

Belfast Data Centre Exit and move to the Cloud

41 IT Strategy is to exit the Belfast Data Centre in 2021 and move Horizon to a cloud based solution. Due to the size, scale and complexity of this move an aggressive timescale has been set. To meet these timescales the migration of data out of the Belfast Data Centre is planned for eight week time.

42 Fundamental to the transition is the management of the risk to the integrity of Horizon data and the implication for Post Office upstream clients such as Government, Banking Services and Bill Payments contracts.

43 It was previously reported that the process of moving Post Office data into a cloud environment with access being granted from outside of the EEA would be challenging. IT, in conjunction with AWS, are deploying a solution where all Post Office data will be encrypted in the cloud with Post Office holding the encryption keys.

44 This means that even if an incidental transfer were to occur that AWS could not access any of the raw data without Post Office releasing the encryption code. This will be an easier sell to our upstream clients who may be nervous about moving into a cloud based solution.

45 IT, Legal and Compliance are working together to deploy a contractual and operational solution that will eradicate the need to consistently seek the approval of upstream clients when personal data may be processed outside of the EEA. Working with external lawyers a compliant solution inside Post Office Risk Appetite has been identified and is currently being developed.

POL00423570

46 This new solution will require the approval of all upstream clients which will be challenging given the aggressive timescales of the migration. However all involved believe this challenge will bring both operational and financial benefits to Post Office and help deliver the CIO's IT Strategy.

Post Office use of Cookies on Internet and Apps

47 The solution for resolving the outstanding Cookies issue has been built and been deployed on the Post Office website.

48 As previously reported to and agreed by the Committee, this solution does not completely address the new consents guidance from the ICO but it does provide strong protection for customers and helping sustain commercial viability. This does position Post Office "in the pack".

49 A recent court case in Germany has ruled that a solution similar to that deployed by Post Office is non-compliant with EU legislation and has taken action against organisations deploying such. The DP team is working with Legal to understand if this ruling has any impact in the UK.

Financial Crime

Compliance with Money Laundering Regulations

50 137 new Bureau de Change cases were identified between 20th April and 19th June 2020 (up 92.9% from the same period in 2019). Most related to low value linked transactions which were deemed suspicious, but there has been a recent increase in higher value Bureau de Change Sell transactions, in line with changes in lockdown rules and international travel.

51 The monitoring report introduced in January to identify branches processing multiple transactions just below the threshold for ID has helped us to take action in 5 branches where transactions have been deliberately split.

52 The solution to extract the correct data for Sanction Screening has been implemented. Due to the downturn in transactions, no sanction hits have occurred, and until there has been a partial/exact match, the solution cannot be effectively live tested. The manual workaround is still in place and has been effective to date.

53 Suspicious Activity Reports and investigations have reached record levels during the lockdown period, with 930 SARs and 159 investigations in April & May (compared to 598 and 84 in April & May 2019).

POL00423570

Anti-Bribery and Corruption ("ABC") update

54 The new reporting and approval portal is live, however, some IT issues have been identified, and some modifications are being developed by IT to resolve. There has been minimal reporting during Covid lockdown.

Whistleblowing Update

55 The migration to the new Navex Global Ltd platform was completed in May, and further communications and awareness are planned during the summer.

56 There has been a slight decrease in new reports in Q1 2020/21, with 8 reports received in comparison to 9 in Q1 2019/20. There continue to be a number of reports against employees at non-customer facing sites (please refer to the Whistleblowing MI in the Reading Room).

57 Two branch related investigations remain on hold as a result of Covid-19 restrictions which is making it difficult to undertake visits, but with the ease in lockdown, these will now be progressed.

Fit & Proper update

58 The agent F&P data was sent to HMRC on 19th June, following an agreed 2 month suspension. 7 data gaps were identified relating to 6 branches that have been in short term temporary closure status for over a year, and these are being investigated.

59 This was the last manual data collation and followed the de-registration of c.6,000 branches that were commercially unviable for Travel Money, or have been temporarily paused as no transactions are currently being undertaken, in order to reduce the cost of annual registration from over £3m to c.£1.3m. HMRC have also deferred payment of the fee from 1st June 2020 until 1st December 2020.

60 There have been two meetings with HMRC to discuss fees. The first was to try and identify a solution that prevented the deregistration of the 'paused' branches, but constraints within HMRC systems and policy meant that a mutually satisfactory solution could not be identified, hence the branches will need to be re-registered if and when the Travel Money business picks up.

61 The second meeting was for HMRC to discuss with Post Office the forthcoming fees consultation, and understand impacts due to the size of our Network. HMRC shared with Post Office the options they had considered and provided explanation as to why a number were unviable. The three remaining options are based around per premises fees, but linked to the National Risk Assessment (NRA). We raised with HMRC that the NRA assess Money Service Businesses as high risk due to the ongoing concerns around money transmitters, however travel money is low risk. We have also asked them to consider a tiered approach to premises fees, e.g. the first 2,000 subject to the highest fee, which would take into account the economies of scale of supervision of large traders like Post Office. Such a solution would also ensure HMRC meets the requirements of 'Managing Public Money Guidance' whereby they must ensure that smaller businesses are not subsidising the supervision or larger businesses. They have agreed to explore these points, and a further meeting is planned in July.

62 The F&P system solution was delivered on 12th June and data migration from the current solution scheduled for completion by end June. The project team is working on processes and controls with Post Office teams to ensure that there are no missing fields from source data for the monthly feeds into the new system. The re-declaration process is due to commence in July, with monthly HMRC reports being driven from the new system from

POL00423570

the July submission. We have written to HMRC and asked that we change the submission date to the fourth Friday each month, and are awaiting their response.

External Threats

63 The National Crime Agency (NCA) published the 2020 National Strategic Assessment of Serious and Organised Crime. It emphasises that UK-based criminals are continuing to introduce criminal cash into the UK banking system. Criminals are utilising money mules, money service businesses, post offices and virtual assets as a means of disguising the origins of their cash as it enters the financial system.

64 Throughout the lockdown period, we have continued to see high levels of suspicious banking cash deposits, and continue to work with the National Economic Crime Centre (NECC) and Project Admiralty (one case involves high value cash deposits made onto multiple banks cards at 45 branches between 18th February and 8th June 2020 totalling c.£7m). A further meeting has been held with the banks in the Banking Framework sub group that is looking at money laundering risks, but there is little progress on identifying control improvements to date. A further meeting is planned for July.

65 We continue to support the Covid Fusion Cell, and a sub group has been established to look at cash based money laundering. Criminals continue to exploit the COVID-19 posing as employees of government authorities and legitimate businesses. Phishing emails and phone calls have involved requesting payment for treatment, fake websites selling testing kits, vaccines and masks. The NECC expects that the UK will see an increase in fraud related to COVID-19 over the coming months, and there is particular concern about the effect that the downturn on the economy will have on criminals being able to more easily recruit mules to launder the proceeds of crime. The Financial Crime team have delivered a number of branch communications to increase branch awareness of scams and COVID-19 related fraud, and further communications are planned.

66 Commerzbank AG (London Branch) was fined £37.8M by the FCA for failing to put adequate anti-money laundering systems and controls in place between September 2012 and September 2017. It is was identified that understaffing of the Financial Crime team within Compliance contributed to the failings, which included identification and treatment of Politically Exposed Persons (PEPs) and transaction monitoring.

Supply Chain Compliance

67 No assessment visits undertaken since March. Awaiting sign off by the Health and Safety team for a re-start date to commence assurance visits - expected to commence in July, provided there is available accommodation.

68 Twice-weekly communications were issued to sites during April and May to help maintain compliance, 12 were issued in total.

69 Weekly compliance activities focussing on specific areas of assurance activity commenced in June and will run until the end of July.

Financial Services

Compliance Monitoring

70 Compliance is currently supporting the business with support and communications on preparing for business re-invigoration in the post lockdown environment.

71 The key resumption of activity will be branch travel insurance sales (potentially in September). This will require compliance oversight of training, awareness and communications (including brochure ware) and eventually monitoring. This will be a significant undertaking particularly with new Covid 19 travel insurance policy restrictions that will need to be disclosed clearly at point of sale.

Confidential

POL00423570

72 Mystery shopping was paused in March. We are planning to introduce a small number of mystery shops from August for POI protection business and it is likely that wider mystery shopping (Boi, Telco) will resume in Q3 including for the re-launched travel insurance business.

73 We continue to maintain governance and regular 'check ins' with our Principals. The normal monthly governance meetings have remained in place albeit with a reduced level of MI.

FS Regulatory updates

74 A summary slide of the key future developments is included in the reading room, a number of planned changes have been delayed whilst the regulator focuses on managing the crisis. The immediate focus from the FCA during Covid 19 crisis has been working with the industry on the well published consumer forbearance measures for credit card, loan and mortgage repayments, these are being delivered through our product partners BoI and Capital One.

75 A key focus area has also been regarding retaining access to cash for the vulnerable particularly as the growth of contactless payment has continued. We await the government legislation on this, but in the meantime the FCA stated in June that they have been working closely with firms to help them move towards reinstating services for customers in a consistent way. The expectation is that firms will prioritise;

76 Where possible, and in line with relevant government guidelines, reinstating access to cash and essential services in local areas which have lost access to bank branches or cash during the crisis.

77 Where it is not possible to reinstate access, and in areas where a reduced service remains, ensuring that there is clear communication to customers through websites and physical signs at branches to signpost to alternatives, such as Post Office services.

Digital Accessibility Compliance

78 The Public Sector Bodies (Websites and Mobile Applications) (No. 2) Accessibility Regulations 2018 come into force for public sector websites including Post Office from 23 September 2020 and PO Mobile Apps from 23rd June 2021. The purpose of these rules is to improve digital accessibility for vulnerable and disabled customers. Post Office will also need to publish an accessibility statement on our website explaining how accessible the site is.

79 The Digital and Innovation team has been working for some time on a programme of work to ensure that we adhere to the standards for key parts of our platforms and experience initially focussing on the website. D&I had also recruited a Head of User Experience and Design with extensive experience in this area.

80 As well as wanting to follow the requirements, we also want to do the right thing to improve accessibility for our vulnerable customers. The charity Scope found in 2019 that 75% of survey respondents felt business was losing out due to poor inclusive design. What's more, when faced with problems using a website or app, 50% of respondents didn't complete the purchase; while 48% found an alternative place to buy – taking their business elsewhere.

81 A detailed paper for discussion will be prepared for the July GE on 15th July.

What is the approach to Compliance?

82 The D&I team have been working with an external accessibility auditor AbilityNet to provide compliance support and to audit the PO website. AbilityNet are established leaders in their field and have worked with a number of large public and private sector firms.

Confidential

POL00423570

83 Working with AbilityNet the D&I team have concluded that it is not currently possible or cost effective to have every part of the site accessible to the same standards by the Government deadline. The Government Digital Service (GDS) states that 'You may not have to meet the requirements for your whole website or app if doing so would be a disproportionate burden - for example, if it's very expensive to make even simple changes and those changes would bring very limited benefits to disabled people'.

84 So D&I have focussed on key areas of our website that will have the most customer interaction and traffic. The D&I team and AbilityNet have confirmed that this approach is consistent with the approach taken by other public sector bodies.

85 The audit has found some issues; many that are commonly found on platforms of our size, age, and complexity:

86 Some pages and parts of the experiences have issues with users' ability to tab through content – For blind or partially sighted users who are unable to use a mouse, it makes using these touchpoints harder.

87 Colour Contrast Issues – Where assets or interactions are layered on top of each other, or close in proximity to one another, a lack of colour contrast makes it hard for visually impaired users to differentiate the individual role of the assets.

88 Marketing Video Content – Videos are not transcribed, making the content unusable for our deaf or hard of hearing customers.

What are the next steps?

89 The audits have raised a significant number of issues, but the intention is to fix as many of them as possible against the audited pages and modules. By doing so we intend to lodge ourselves, with backing of AbilityNet our third party auditor, as partially compliant as opposed to fully compliant, because we've focused our attention on a series on significant touchpoints on our website, as opposed to the entire digital product, for the reasons outlined above.

90 We also plan to involve user testing from the charity sector on our improvements, this will send a powerful message about our intent and wanting to do the right thing rather than just comply. This is something PO did with the Travel App when it was being developed using accessibility champions at the charity Sense.

What are the risks of being partially compliant as opposed to being fully compliant?

91 The GDS will examine a sample of public sector websites every year. GDS can ask for information and request access to intranets, extranets or any public sector website. Significant non-compliance could be seen as a breach of the Equality Act 2010 and the Disability Discrimination Act 1995.

92 However, PO has a credible work plan in place with improvements made and in progress, including the use of external accessibility experts and expected involvement and support with the charity sector.

What about the App and other POL digital touchpoints?

93 Legislation dictates that we have until 23rd June 2021 to meet compliance for any mobile applications, and hence on completion our web accessibility programme, the D&I team will be conducting the same activity against the app to meet that deadline.

Mails – Dangerous Goods

94 Please refer to the separate paper included in the Reading Room. This paper sets out in detail the actions being worked on by the Mails and Network Teams.

POL00423570

Internal Audit

Summary of Control Themes for 2019/20:

95 During 2019/20 Internal Audit raised a total of 171 audit actions across 25 audits (compared to 271 actions across 24 audits in 2018/19). The lower number of audit findings indicate a general improvement in the control environment.

96 Audit findings were analysed to identify recurring control themes and root causes. The top five control themes were as follows, with full results included in the reading room (app. 8).

Control Theme (by COSO control components)	% of Audit Findings		
	19/20	18/19	
Change Delivery[1]: Ineffective change governance, risk management and tracking / realisation of benefits.	31%	44%	↓
Control Activities: Internal controls are not deployed through policies, procedures and systems and / or internal controls are not designed or operating effectively.	22%	15%	↑
Risk Assessment: Ineffective identification and/or management of operational, financial and information risk (including unclear expression of risk appetite).	13%	5%	↑
Information & Communication: Unavailability of relevant, quality information to support the internal control function and decision making.	8%	12%	↓
Monitoring Activities: Oversight and governance groups are not effective in identifying and correcting control weaknesses.	6%	3%	↑

[1] Change Delivery is not a standard COSO control component, however, these findings are shown separately to avoid distortion of BAU controls.

97 The year-on-year movements in control themes can be summarised as follows:

- Change Delivery: There was a notable improvement in the effectiveness of Change governance and controls. A significantly lower number of control failings were identified compared to the previous year (53 vs 118), from a similar number of reviews performed. The reorganisation of the Strategic Portfolio Office (SPO) and appointment of a new Chief Transformation Officer in 2019, together with the adoption of a Change Excellence Framework have laid the foundations for a stronger control environment driven centrally by the SPO. A detailed Change Controls Framework has also been developed, and although this is still being embedded, there is already a noticeable improvement in the consistency and effectiveness of controls operating at programme level.
- Control Activities: The percentage of audit findings relating to ineffective control activities has increased by 7 percentage points, indicating reduced effectiveness of core internal controls and is a regression from the 18 percentage point improvement reported the previous year. Our audits have noted that control activities did not always keep in step with organisational and system changes, however, we highlight that appropriate remediation was implemented when control failings were identified. We will assess the role of the second line of defence activities to monitor first line controls operation – there are 3 reviews of the second line on the FY20/21 plan.

POL00423570

- Risk Assessment: Operational risk management was less effective compared to the previous year (findings increased from 5% to 13%). Risks were not always proactively identified, remediated and escalated.
- Information & Communication: There has been an improvement in availability of relevant, quality information to support the internal control function and decision making (down to 8% from 12%). The standard of policies and procedures continue to improve, with more effective communications to raise awareness of new or updated policies.
- Monitoring Activities: Although this represents a low number of findings (10 instances or 6% of total findings), the year on year deterioration indicates that oversight and governance groups have become less effective in identifying and correcting control weaknesses. This could be a consequence of staff churn, especially at a senior level where monitoring activities will typically be led and challenged by more experienced managers.

Audit report turnaround performance for 2019/20

98 The average time to clear internal audit reports during 2019/20 was 30.85 working days against the target of 20 days. This is a significant improvement on the previous year's turnaround time of 41 days. The improvement was achieved despite the delays experienced in the clearance of the final three reports for 2019/20 due to the impact of Covid-19.

Progress against Internal Audit plan

99 At the time of the May ARC meeting, the last audit from the 2019/20 internal audit programme was still being finalised. This report (FS Branch Sales) has since been completed and a summary is included in par 103.

100 In response to the Covid-19 crisis, a re-prioritised Internal Audit programme was approved at the May ARC meeting. It was agreed that a more dynamic (quarterly rolling) audit plan will be adopted and reviewed at each ARC. Progress against the Q1 plan is shown in the table below with the full plan in the reading room (app 15):

	Review	Status & Timing
POL		
1	Covid-19 Programme Assurance	Fieldwork complete. One interim report issued, final report in draft. In addition Deloitte delivered 3 insight reports to ARC.
2	Maintain Minimum Control Standards	Two interim reports issued (Cash Controls and Financial Reporting Controls). Third and final phase (IT Controls) nearing completion (10/7).
3	Cyber Security Maturity	Interim report issued covering Covid-19 response. Final report in draft.
4	Health & Safety response to Covid-19	In progress (30/6 – 30/7).
5	Effectiveness of Second Line during Covid-19	Interim report issued. Phase 2 (deep dive) in progress (12/6 – 30/7).
POI		
6	Data: Governance, ethics, privacy & security	Phase 1 underway to assess 3rd Party Data Security Risks.
7	Cyber Security (POL-POI Gap Analysis)	In progress. Fieldwork nearing completion (17/6 - 14/7)
8	Incident and Breach Management	In progress (17/6 – 17/7)

POL00423570

101 The following audits are being planned for delivery in Q2:

	Review	GE Sponsor	Timing
1	GLO Operations Improvement Programme (Common Issues Judgement)	Al Cameron	Oct
2	DB Pension Scheme Data Errors	Lisa Cherry	July
3	Postmaster Reporting (MI, Branch Trading Statements)	Amanda Jones	Sept
4	GLO Historical Shortfall Scheme - Data Validation	Amanda Jones	July
5	Controls over Revenue Adjustments	Al Cameron	Aug
6	Branch Hub (Programme Assurance)	Al Cameron	Sept

Internal Audit reviews completed

102 The following six audit reports were issued since the May ARC meeting:

1	FS Branch Sales (FY20 IA Plan) (Final Report)		4	Minimum Control Standards – Ph2 Financial Reporting Controls	
2	CV-19 Programme Assurance - Ph1 Set-up & Governance		5	Cyber Security Maturity Assessment	
3	Minimum Control Standards - Ph1 Cash Controls		6	Effectiveness of Second Line during CV-19 – Ph1	

103 Our findings and observations from these reports are summarised below, with the full reports available in the reading room (appendices 9-14).

1. **FS Branch Sales** (Ref. 2019/20-25)



Sponsor:
Owen Woodley
Audit actions:

P1	0
P2	0
P3	1
Total	1

Appendix 9

The objective of this review was to assess the adequacy and operating effectiveness of controls to ensure that promotional materials offered and activities done at branch in support of FS product sales are compliant with the AR agreements and the related regulatory requirements.

We conclude that the mechanisms in place to assure branch sale compliance, are operating as described, which enables Post Office to meet its contractual obligations to its Principals. IA noted significant improvements in the processes and controls operating when compared with those reviewed previously in FY16/17. In addition, we highlight that the risk exposure has been reduced since FY16/17 as sales activities are now limited to a subset of PO Money products, along with travel and some protection insurance sold on behalf of POI. We noted an opportunity to review Post Office's assurance approach to ensure it remains fit for purpose and is done in a cost effective way.

Management Comment

We welcome the satisfactory rating and will continue working with our principals, network and compliance colleagues to ensure our mechanisms and approaches remain as effective as they can be.

Chrysanthy Pispinis – Post Office Money Director

Network welcomes the findings and recommendations of this report. As a result of the new field team structure implemented in March 2019, which extended our reach to all physical branches, the network has significantly strengthened its Financial Services compliance awareness.

Andy Kingham – Head of Network

I am pleased the review recognises the strengths in Compliance's oversight of FS branch activity and the approach taken. We continue to develop our approach to oversight and this will include any changes required to support the developing branch distribution strategy.

Jonathan Hill – Compliance Director

POL00423570

2. **Covid-19 Response Programme - Phase 1** (Ref. 2020/21-06)	
 ***Sponsor:*** *Nick Read* Management comments and audit actions will be in the final report at the end of phase 2. *Appendix 10*	Following the Business Protection Team's early mobilisation and crisis response to the pandemic during February & March 2020, the Covid-19 Response Programme was established. The programme was key to formalise the management of the next stage crisis relief activities, ensuring their sustainability for an extended period of time. Phase 1 of the review assessed the Programme Set-up and Governance. We concluded that the set-up and management of the Covid-19 programme has been effective in driving Post Office's mobilisation and crisis response activities. It has effectively concentrated efforts to collect key insights and to coordinate activities needed to achieve Post Office objectives to keep the branch network open, protect the workforce, customers and supply chain, and maintain effective communications throughout. We found that the programme was well-structured overall with clarity in regards to roles and responsibilities. The daily rhythm of functional, operational and governance meetings increased the flow of information to all levels of leadership, and ensured it was well disseminated to drive collaborative and coordinated next steps.

3. **Minimum Control Standards (Ph1) Cash Controls** (Ref. 2020/21-05)	
 ***Sponsor:*** *Al Cameron* Management comments and audit actions will be in the final report at the end of phase 3. *Appendix 11*	The purpose of this audit was to consider the impact on key controls from changes in processes as a result of operational challenges arising from Covid-19, and to ensure that minimum control standards are operating effectively. Phase 1 of this review assessed controls over cash processes. We have rated this report satisfactory, having concluded that controls over cash were appropriate in the circumstances and continued to operate effectively during the response to Covid-19. From the outset, Supply Chain knew it would be affected by staff absence due to shielding, self-isolation and sickness, which at its height reached up to 30%. New controls with contingency suppliers were put in place to ensure the distribution of outbound cash and the reconciliation of inbound cash could be processed in a timely fashion. This involved working with both Loomis and NatWest to agree the level of services and ensure adequate levels and standards of control could be applied to all processes. Good collaboration across businesses and teams enabled this to be done very quickly and the contingency arrangements were working within the first two weeks of April. Supply Chain also introduced a risk based single-pass check for processing of inbound remittances to enhance productivity (resulting discrepancies are being closely monitored). A request from DWP to send cash to the most vulnerable of POCA customers was responded to with similar efficiency, using Royal Mail Special Delivery. Controls have been devised and implemented to ensure this service can be offered securely and on demand whilst safeguarding the personal data of vulnerable customers. Controls over the normal cash processes have been operating as designed throughout the crisis with minimal interruption. Where changes have been necessary to accommodate remote working these have been defined, agreed, signed off appropriately and implemented. The audit highlighted a need to improve controls documentation and audit trail.

POL00423570

4. **Minimum Control Standards (Ph2) Financial Reporting Controls** (Ref.2020/21-05)	
 Needs Improvement ***Sponsor:*** *Al Cameron* Management comments and audit actions will be in the final report at the end of phase 3. *Appendix 12*	The purpose of this audit was to consider the impact to key controls from changes in processes as a result of operational challenges arising from Covid-19, and to ensure that minimum control standards are operating effectively. Based on our work to date, we conclude that the control environment relating to Financial Reporting has been maintained throughout PO's response to the Covid–19 crisis, albeit with challenges around formally evidencing control activity. Controls have been operated as if in BAU for the most part and only amended where absolutely necessary to accommodate the challenges of a remote working population. The control self-assessment process has been maintained throughout, although there were access issues with TrAction that delayed the evidencing of controls operation for April. This has now been resolved. We further highlight opportunities to improve controls over Agent Expenses and Payroll processes that were designed to operate in the office environment, particularly in relation to evidencing checks and manager authorisation. These controls have had to be adapted for the remote working environment, but do not permit an adequate audit trail to be maintained. Management are implementing MS Teams to evidence control activity and retain audit trail.

5. **Cyber Security Maturity Assessment** (Ref.2020/21-02)	
 Needs Improvement ***Sponsor:*** *Jeff Smyth* Audit actions: P1 4 P2 4 P3 0 Total 8 *Appendix 13*	In 2018/19, Deloitte, in partnership with Internal Audit, carried out a comprehensive review of Post Office's cyber controls across 34 cyber capabilities. The objective of this review was to re-assess the maturity of controls in place to protect the confidentiality, integrity and availability of POL's infrastructure, systems and data. Significant work has been carried out over the last year to rationalise the cyber operating model and enhance controls, especially those which protect data and identify threats and vulnerabilities. Policies and standards now better reflect the individual controls needed to meet requirements, POL's ability to capture and act on threat intelligence is greatly enhanced, and progress has been made on managing the identity lifecycle through integration of HR and IT systems. However, we highlight that further work is required to meet target maturity levels and there is a need to develop and document a comprehensive strategy and architecture to support the deployment of cyber security. This should be focused around an agreed set of Crown Jewels and lead into an end-to-end cyber programme. We have rated this report '**Needs Improvement'** reflecting the progress made against the maturity targets and an assessment of the degree to which cyber risks are mitigated by the current controls.
Management Comment provided by Tony Jowett (CISO) This review has been focused on the areas where we believe we have made some progress positively and also where we are highlighting areas that need further activity. The review scores, the comments associated with them and the development activity highlighted are fair and accurate.	

Confidential

POL00423570

6. **Effectiveness of the Second Line (Ph1)** (Ref.2020/21-07)	
Not Rated ***Sponsor:*** *Al Cameron / Ben Foat / Jeff Smyth* Management comments and audit actions will be in the final report at the end of phase 2. *Appendix 14*	The objective of this review is to assess if key second line assurance activities continue to operate effectively during the Covid-19 crisis. Internal Audit have completed an initial assessment of the impact of Covid-19 on 12 second line assurance activities in Post Office. Results from our initial assessment indicate that all second line functions continued to operate effectively throughout the Covid-19 crisis. Teams are able to work remotely, have clear priorities and are generally positive about their interactions with the business, senior and external stakeholders. However, some teams are facing significant additional challenges and will be subject to a more in-depth review to understand if and to what extent their effectiveness has been impaired. Based on the results of phase 1 of this review we will perform a more in-depth review of the following five second line activities: Loss Prevention, Financial Crime, Compliance, IT Security and Health & Safety.

Status of Audit Actions

104 Audit actions are generally being completed on time. However, we highlight that the changes to business priorities due to Covid-19 have caused delays in completion of some audit actions. We have been working with the action owners and GE sponsors to agree revised completion dates for 14 actions, 6 of which remain open and are now overdue.

105 The movement and ageing of audit actions are shown in the table below (status at 7 July 2020).

Audit Action Status (POL):	
Open actions at last ARC	54
Less: Actions closed in period	29
Add: New actions in period	13
Total open actions	**38**

Ageing:	
Open (not yet due)	30
Overdue (<60 days)	8
Overdue (>60 days)	0
Total open actions	**38**

106 The reasons for the 8 overdue actions are as follows:

- **Belfast Exit** – 6 actions were delayed due to Covid-19. These actions are now being addressed following the approval from IC to continue with programme delivery. Internal Audit will review the actions as part of our planning of the next phase of the programme (Action owner – Rob Wilkins).
- **Investment Funding Follow-up Review** – 2 actions are overdue; 1 was delayed because of capacity constraints related to Covid-19 and the other due to it taking longer to find a suitable solution (Action owner – Max Jacobi).

POL00423570

Appendices[1]

Central Risk

Appendix 1: Enterprise, Intermediate and Risk Register Dashboards
Appendix 2: Change Portfolio

Compliance

Appendix 3: Prohibited Restricted Items
Appendix 4: Covid-19 Dashboard
Appendix 5a: Compliance Dashboard
Appendix 5b: Compliance Dashboard
Appendix 6: Telecoms Regulatory Calendar
Appendix 7: FS Regulatory Calendar

Internal Audit

Appendix 8: 2019/20 Internal Control Themes Summary
Appendix 09: Internal Audit Report – FS Branch Sales
Appendix 10: Internal Audit Report – Covid-19 Programme Assurance (Ph1)
Appendix 11: Internal Audit Report – Minimum Control Standards (Ph1) Cash Controls
Appendix 12: Internal Audit Report – Minimum Control Standards (Ph2) Financial Controls
Appendix 13: Internal Audit Report – Cyber Security Maturity Assessment
Appendix 14: Internal Audit Report – Effectiveness of Second Line during CV-19 (Ph1)
Appendix 15: Internal Audit Plan for 2020/21

[1] Appendices are accessible in the CoSec 'Reading Room'

Confidential

POL00423570

POST OFFICE LIMITED
RCC REPORT

Title:	PCI DSS Compliance	**Meeting Date:**	13th July 2020
Author:	Joseph Moussalli, PCI DSS Programme Manager	**Sponsor:**	Jeff Smyth, Group Chief Information Officer

4

Input Sought: For Noting – please note risks.

RCC is requested to note:
What programme progress has been made during the last reporting period?
What are the key risks?

Previous Governance Oversight

There is a rolling requirement for PCI to be on the agenda.

Executive Summary

The current programme plan delivers Ingenico banking software Vocalink accreditation by December 2020, completion of software deliverables testing by February 2021 and to complete pilot by late March 2021. Branch rollout will be completed in May 2021 and formal PCI-DSS accreditation will be achieved by June 2021. The programme is currently tracking on schedule but there are some risks identified that are discussed in the paper.

The main achievements / status since the last update are listed below.

Board authorisation giving a total funding of £15.8m was provided on 26th May 2020. This approval provides additional funding of £7.2m to progress the programme through to completion.
Drawdown of £4.6m to allow the software development to be funded to January 2021 was agreed at IC on 6th July 2020.

Fujitsu contract CWO230 approved by all parties on 8th June 2020. New interim critical milestones have been agreed to ensure that Fujitsu and Ingencio demonstrate progress of the payments and banking development.

Ingenico & Post Office PCI DSS Executive Meeting (Nick Read and Jeff Smyth) was held with the Ingenico Group CTO Paula Felstead and a renewed commitment was provided by Ingenico to achieve Vocalink Accreditation by the end of December 2020.

The Banking forum has been updated with a plan showing 2021 dates for the first time and indicating Pilot and Branch rollout commencing in February 2021.

IT workstream

- The Retail Payments release is on track and an early POS simulator demo has been provided. Ingenico is validating Retail Payments transactions with Global Payments in advance of formal accreditation and the software is on track to be ready for pilot on 23rd October 2020.
- The Banking Transactions release is also on track. Ingenico is working towards a balance enquiry demo on 31st July and to achieve Vocalink accreditation due by Dec 2020.

Confidential

POL00423570

- PED branch upgrades (new firmware and installation of Ingenico EMV and banking keys) resumed on 1st July 2020 and we have now completed 19,182 of 24,500 PEDs (78%) to 3rd July 2020. This activity is on track to complete at the end of September.
- POCa PIN change deployment 70.12 completed. POCa users are now able to change their PIN at a counter.
- Several items not included in the current Fujitsu (Ingenico) development have been identified as essential for the go-live and /or audit. These may impact the plan if they cannot be accommodated. (Processing of banking BIN ranges greater than 6 digits, ePortal requirements for FCT, Counter training)

Target Operating Model (TOM) workstream.

- There are now seven TOM delivery releases - two of these releases are dependent on the P2PE solution release. One release has been de-scoped – Santander Credit Card Bill Payments.
- TOM work is currently tracking to plan however there is still scope /cost / timeline risk and therefore significant focus is being placed on this activity.
    - Release A – Obfuscation of PAN numbers on screens and receipts is in test.
    - Release B –Telephony payments – Purchase Order placed with Verizon.
- Several TOM remediation items are still in analysis or design (TMC, Pre-paid cards, Financial Crime Investigations, O365 /Mimecast).

Questions addressed

1. What has been the progress since the programme last presented in May 2020?
2. What are the key risks on the programme?

Report

1. What has been the progress since the programme last presented in May 2020?

Enhancement to Programme Plan.

The overall programme is scheduled to complete final banking software deliverables from Ingenico in early February 2021 and to commence branch rollout in March 2021. Branch rollout will be completed in May 2021 and formal PCI DSS accreditation will be achieved by June 2021. The plan has been brought forward two further weeks.

We have agreed interim critical milestones in the CWO with Fujitsu / Ingenico to track progress:

Milestone	Delivery Date
Ingenico C3 API specification for the banking release (key delivery milestone).	Delivered
Balance Enquiry transaction demo on Ingenico test bed	31st July 2020
Ingenico to provide code to enable a cash withdrawal transaction	30th September 2020
Fujitsu end to end cash withdrawal from PED/POS to Vocalink	19th October 2020
EMV Retail ready for live pilot	23rd October 2020
Vocalink accreditation completed	December 2020 (brought forward from 18th Jan 2021)

POL00423570

Milestone	Delivery Date
Ingenico Development and End to End Testing Complete	31st January 2021
POL UAT Complete	16th February 2021
Production Complete and ready for Pilot	3rd March 2021

The programme plan is shown in Appendix 1.

There is a new risk that additional essential changes are needed to the Fujitsu / Ingenico software that will impact the timeline. Suppliers are indicating that they are unable to accommodate these essential changes within the required timescales.

IT Workstream Update

2. Summary of key IT activities delivered to date:

The IT workstream P2PE solution will be delivered in the following releases.

Release 1: Payment release (card payments) – technical Pilot for 5 counters in a multi-counter environments.

Release 2: Banking capability introduced – all systems live ready for the branch rollout.

Release 3: Branch rollout of POS and PEDs for both Card Payments and Banking Transactions.The audit will be completed once the POS and PEDs have been updated at the last branch. We have identified some further clean-up tasks that will be needed

The following progress has been made since the last update.

- **PED Upgrade (firmware upgrade and installation of EMV and banking transaction keys):** Completed 78% (19,182 of 24,500 PEDs) of the rollout across POL estate. Deployment was paused on 25th March due to Covid-19 and has just re-started on 1st July 2020. New contract agreed with ComputaCentre (Allvotec has replaced Bybox as a sub-contractor).
- **New Ingenico Point to Point Encryption technology solution for card payments and banking transactions:**
  - **Retail Payments development:** tracking to plan as reported by Fujitsu and Ingenico. The retail payments development is undergoing pre-accreditation testing with Global Payments. A demo using a POS emulator has been provided to Post Office. Fujitsu are building out the counter functionality and have completed the second of five sprint cycles.
  - **Banking transactions development:** Ingenico have completed some of the foundation development. They have been able to prove an application level connection to the Vocalink test system including login, key exchange and balance enquiry without a PIN. Balance enquiry to be demonstrated at the end of July. Ingenico has also brought forward functionality (withdrawals, reversals) from SI22 to SI 21 to attempt to complete Vocalink accreditation by December 2020.
- **Vocalink** are actively supporting Ingencio with integration and understanding the Vocalink accreditation
- **POS Test Counter operating at the Ingeico offices at Dalgety Bay:** Ready for Ingenico Global Payments accreditation.
- **TMS tool for chain of custody –** PED data now being re-loaded by ComputaCentre (Allovtec).

POL00423570

- **Santander Bank Giro processing through the Ingenico/Vocalink solution:** Discussions ongoing with Santander about the Design & implement the migration of the Santander transaction data link to Vocalink. Progress is slow but we have engagement and the Exec level are aware that this is a must do compliance programme for the Post Office.
- **POCa transaction routing through the Ingenico /Vocalink:** Design & implementation of the migration of POCa transaction data link and messaging from/to Vocalink is in progress and we are expecting a firm proposal from DXC by mid-July 2020.
- **POCa PIN change –** bug fix rolled out to the branch network.
- **Service readiness:** Building the Service Wrap (incorporating the Service Modelling, Design, Build and Run)

Target Operating Model (TOM) Workstream Update

3. The focus of the Target Operating Model workstream is to review the Products and Processes that use Card Holder Data and to remediate and remove them from the scope of the PCI DSS audit where possible. If this is not possible then PCI DSS controls will be put in place. A plan has been prepared to remediate the products and processes. However, as analysis is still ongoing in some areas (see the list below) so there is still some uncertainty in the costs.

4. Current planning indicates all product and process remediation can be completed within the P2PE delivery timeframes. The following tasks have been achieved in this period:
   - The TOM plan has been substantially updated and reviewed.
   - Eight TOM releases were identified last time, (one of which has now been de-scoped) and two of these depend on the P2PE solution.
     - Release A: PAN on screen and receipt obfuscated. This release is now in UAT.
     - Release B: Telephone payments. Contract agreed and PO raised with Verizon for PCI PAL solution. Voice recordings to be deleted - speech analytics no longer required.
     - Release C: Obfuscation of CHD in Fujitsu data centres remediated. Fujitsu has provided a paper with some options but some systems have immutable data and these will need to be managed under PCI controls.
     - Release D: Travel money card top-up process remediated. A solution design has been proposed to Fujitsu and they are providing a quotation.
     - Release E: Fujitsu back end reconciliation process adjusted.
     - Release F: Quatrix – process for CHD. TOM is remediating the processes for placing data on Quatrix. A 14 day data retention period is being implemented. One off scans will be implemented to discover and remediate any processes that continue to transfer CHD in Quatrix. Mimecast DLP is being evaluated to see if it can be used for detection and blocking of transmission of PAN data.
     - Release G: Financial Service and Financial Crime team process adjusted.
     - Release H: Payment of Credit Card Bill Payment (Santander) (De-scoped)

   Key areas of the TOM workstream and the status of the items that are still in analysis or design are:

   - Financial Crime Team / Financial Service Centre team payment investigations. Discussions ongoing with Fujitsu /Ingenico about a solution for the banks.

Confidential

POL00423570

- Data network scanning – the remediation approach is being discussed with the Compliance team. Evidence is still being traced – further costly scans may still be needed.
- Pre-paid credit cards – top-up solution required. This is needed for go-live but not currently in the Fujitsu /Ingenico development stack.
- Travel Money Card top-up – three solutions being evaluated. This is needed for go-live but not currently in the Fujitsu /Ingenico development stack.
- Reconciliation design (post P2PE implementation)
- Data retention and legacy conditions being evaluated with Fujitsu.

A dashboard illustrating the scope, supplier involvement and timelines can be found in the Appendix 2.

Financial Impact

5. The programme forecasts it will need £15.8m funding through to completion. The phasing of this expenditure by FY is captured in the table below.
Programme costs are currently tracking to plan and details are provided in Appendix 4.

Risk Assessment, Mitigations & Legal Implications

The following are identified as key risks – other managed risks are in Appendix 3.

6. ***Risk:*** There is a risk that additional essential changes are needed to the Fujitsu /Ingenico software that will impact the plan timeline. Fujitsu and Ingenico have given a commitment to meeting the current timescales on the basis of no further changes. Suppliers are indicating that they will not be able to accommodate these essential changes within the required timescales. Essential new development is needed for example to process BIN ranges greater than 6 digits, Pre-paid card top-ups, Travel money card top-ups, ePortal requirements to support financial crime investigations.

Mitigation: Post Office is conducting further analysis with suppliers and compliance to mitigate the risk to the programme timescales and costs. Post Office will also consider if some of the required changes can be delivered as a later release.

7. ***Risk:*** There is a risk that Mimecast DLP alerting and blocking of CHD transmission cannot be implemented in time.

Mitigation: Post Office team is discussing this with security and IT to find a way forwards.

8. ***Risk:*** There is a risk that JPM (DXC) cannot migrate POCa payments to route through Vocalink within the timescales.

Mitigation: Post Office team is working closely with DXC to extract a proposal –costs and timescales. A contingency solution that requires Ingenico development has been tabled but this is also likely to cause delays.

9. ***Risk:*** There is a risk that Santander cannot migrate payments to route through Vocalink within the timescales.

Mitigation: Post Office team is working closely with Santander to extract a proposal – costs and timescales.

POL00423570

Stakeholder Implications

Branch/Client Communications (Comms) Update

10. Continued successful regular client update sessions have taken place with Post Office's acquirers - Global Payments, MasterCard Visa and American Express and WHSmith. The regular client update session will provide them with a forum and information to help manage our key messages with their internal stakeholders.

    PCI DSS auditor: We are also in regular communication with Nettitude, Post Office's quality security assessor (QSA) to keep them updated on progress.

    Positive feedback was received from all parties regarding the approach that Post Office is taking.

    The regular client update pack has been presented to the banking framework partners during the monthly operation forum. The banking forum have been told about our plans to start pilot in February 2021. A series of interim milestones have been shared with the banks to build up credibility in delivery.

Next Steps & Timelines

11. The programme will continue to deliver according to the programme plan – see Appendix 1 and to mitigate risk.

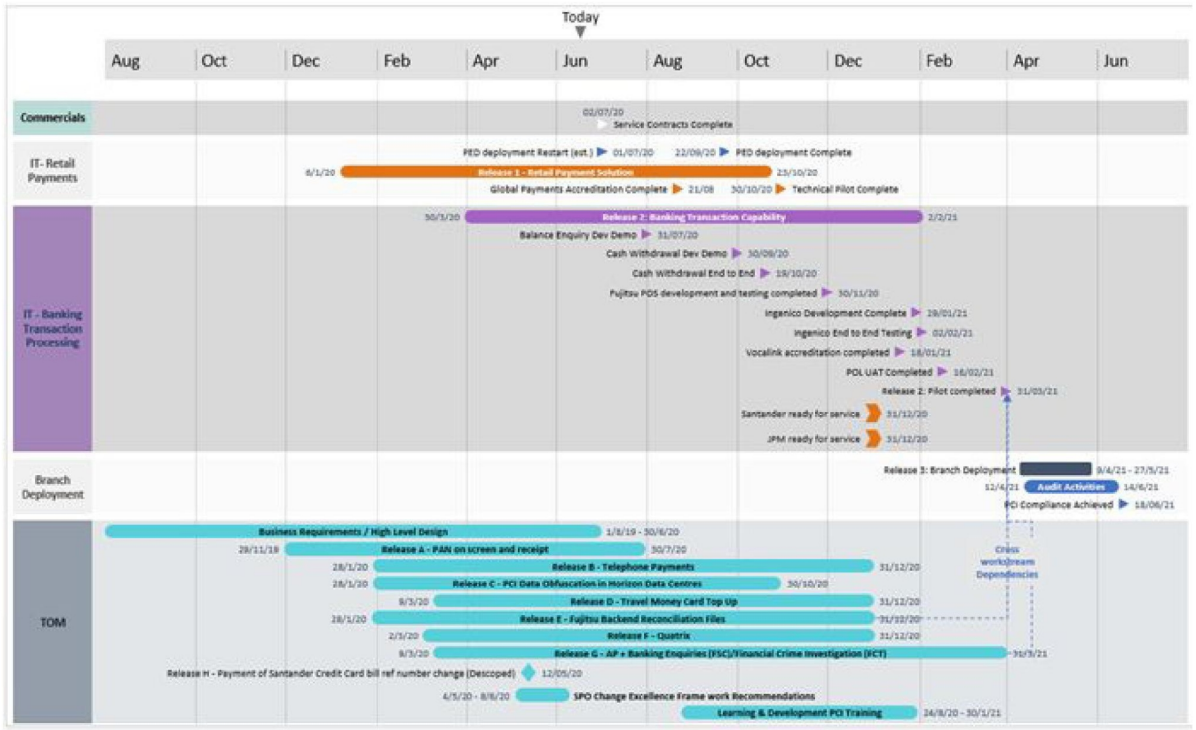
Confidential

POL00423570

4

Appendix 1

Programme plan



The programme plan has been brought forward 2 weeks since the last report.

Confidential

POL00423570

Appendix 2

TOM Workstream Dashboard

	Name	Complexity	Suppliers & Commercials									End-to-End Delivery						
			IUK	FJ	CC	VL	ATOS	Verz	Global	AMEX	FRES	Sant.	Discovery	Design	Build	Test	Service Readiness	Deploy	Complete
	PS1: Bank of Ireland (cc is decommissioned)	M		X			X						03/12/2019	23/03/2020	15/05/2020	26/06/2020	01/07/2020	24/07/2020	13/08/2020
	PS1: Payment of Santander Credit Card Bill (de-scoped)	M		X			X					X	03/12/2019	23/03/2020	15/05/2020	19/06/2020	24/06/2020	16/07/2020	13/08/2020
	PS1: Budget Card (de-scoped)	M		X			X						03/12/2019	23/03/2020	15/05/2020	19/06/2020	24/06/2020	16/07/2020	13/08/2020
Release B: Telephony	PS1: Telephone Payments and Refunds	M							X	X			29/01/2020	19/06/2020	09/10/2020	29/10/2020	04/11/2020	19/11/2020	17/12/2020
	PS2: Storage of Telephone Recordings	H											30/01/2020	19/06/2020	TBC	TBC	TBC	TBC	TBC
Release C: Data Obfuscation in Horizon DCs	PS1: Storage of PCI data in Horizon Data Centres	H		X			X						31/03/2020	26/06/2020	14/09/2020	09/09/2020	14/09/2020	01/10/2020	29/10/2020
Release D: Travel Money Card	PS2: Travel Money Card Top Up	H		X			X			X		X	03/03/2020	19/06/2020					
Release E: Fujitsu Back End Reconciliation Files	PS1: Amex, Vocalink and GP obfuscation	L		X		X	X			X	X		11/03/2020	26/06/2020	15/05/2020	12/06/2020	03/06/2020	03/07/2020	03/07/2020
	PS2: Removing PAN data from PODG, TES, DRS, BRSS, BRDB (CWO226)	H		X			X						11/03/2020	26/06/2020					
Release F: Quatrix, Mimecast, Email	PS1: Transmission and storage of PCI data	M		X									11/03/2020	26/06/2020					
Release G: AP Enquiries, Banking Enq + FCT	PS1: Full PANs used during transaction enquiry searches	M	X										28/01/2020	26/06/2020	*29/01/2021	08/03/2021	23/03/2021	30/03/2021	27/04/2021
	PS2: Full PANs transmitted to and from Banks and clients	M	X											26/06/2020	*29/01/2021	08/03/2021	23/03/2021	30/03/2021	27/04/2021
Other	File Data Storage (Previously Network)	L		X									31/03/2020	26/06/2020					
	POL SAP Archives (potential to de-scope)	L		X									31/03/2020	26/06/2020					
	Credence (to be de-scoped)	L		X									31/03/2020	26/06/2020					
	POL Forms, documents and branch receipts	M		X									31/03/2020	26/06/2020					
	AP-ADC Script Gaps	L		X			X						31/03/2020	26/06/2020					
	Atos Test Environments	L		X			X						31/03/2020	26/06/2020					
	SPO CEF Recommendations	L											31/03/2020	26/06/2020					
	Learning & Development Training Materials	L											31/03/2020	26/06/2020					

Complexity Key		
	# Changes	# of 3rd Parties
Low	0-1	0-1
Medium	2-4	2-3
High	>5	>3

Suppliers & Commercials Key	
RAG Status	Commercials Status
Red	Commercials are delayed
Amber	Risk of Delay to Commercials
Green	Commercials are on track
Blue	Commercials have been agreed/signed
Grey	Commercials have not started

End-to-End Delivery Key	
RAG Status	Delivery Status
Red	Delivery is outside of tolerance
Amber	Delivery is at risk of moving out of tolerance
Green	Delivery is on track
Blue	Delivery has been completed
Grey	Delivery has not been started

Confidential

POL00423570

Appendix 3 other risks currently being managed

12. ***Risk:*** Risk of loss of confidence by our client base should a delay occur.

    Mitigation: Pre-emptive conversations have already taken place with client-facing senior Post Office stakeholders to formulate a strategy should a delay need to be communicated. July update: An external communication in June was made to the banking forum about the banking pilot commencement in February 2021.

13. ***Risk:*** Risk of the solution provider encountering complexities while developing the new solution as this is a new venture for them.

    Mitigation: Post Office has requested Ingenico to provide granular level reporting to allow close monitoring of progress. Therefore, if there are any blockers encountered they can be discovered and addressed quickly.
    July update: Post Office identified critical functionality needed for Vocalink accreditation. This was raised at multiple levels, Ingenico has validated the functionality needed for Vocalink accreditation and realigned this functionality to SI21.

14. ***Risk:*** Risk of Coronavirus may impact the delivery timescales for any supplier across the entire PCI programme. The outbreak of Coronavirus is a global risk event and the overall impact for the programme is not fully evaluated. Consequently, there may be a delay to the some or all of the agreed deliverables which could affect the build or deployment programme stages.

    Mitigation: Post Office is working with all engaged suppliers to better understand their contingency plans to ensure that delivery momentum is maintained. This includes the examination of options to minimise delivery impact by understanding key delivery person risks, supply chain risks and other indirect or latent dependency factors.

15. ***Risk:*** There is a risk to the programme timescales and costs that that post branch rollout clean-up activities may be needed on legacy data. This may include deleting legacy data, awaiting for it to be rolled-off or in certain cases putting PCI DSS controls in place. Known areas of risk include Audit SAN, Transaction Enquiry Service, CC audit log (INTrust), call recordings.

    Mitigation: Post Office is conducting further analysis with suppliers and compliance to mitigate the risk to the programme timescales and costs.

POL00423570

Appendix 4 Funding summary

PCI Programme Capex & Exceptional Spend (2018-2022)	2018/2019 (Act)	2019/20 (Act)	2020/21 (F/Cast)	2021/22 (F/Cast)	LIFE
Internal Labour	-£4,818	£147,407	£544,862	£199,974	£887,425
External Labour	£108,334	£908,887	£482,010	£92,212	£1,591,442
3rd Party Costs	£108,488	£3,613,127	£8,782,999	£667,072	£13,171,685
Exceptional Costs	£65,643	£49,357			£115,000
Actual / Forecast	**£277,646**	**£4,718,777**	**£9,809,871**	**£959,258**	**£15,765,552**
3rd Party Costs Comprise					
Fujitsu	£4,487	£1,950,730	£6,180,884	£402,236	£8,538,336
Computacenter UK Ltd	£0	£1,342,114	£527,046	£115,191	£1,984,352
Atos	£0	£202,011	£399,284	£112,815	£714,110
Vocalink	£0	£36,923	£346,067	£1,824	£384,815
Other	£104,001	£81,349	£1,329,717	£35,006	£1,550,073
Actual / Forecast	**£108,488**	**£3,613,127**	**£8,782,999**	**£667,072**	**£13,171,685**

Confidential

POL00423570

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE

4

Title:	Cyber Security Strategy Update	**Meeting Date:**	13 July 2020
Author:	Tony Jowett, Chief Information Security Officer	**Sponsor:**	Jeff Smyth, Interim Group CIO

Input Sought: Noting

- To note the Deloitte Cyber Maturity assessment findings
- To note the impact of COVID-19 on user behaviour and our plans to address this

Previous Governance Oversight

- Actions to report on the second point above occurred at the previous Risk and Compliance Committee (RCC) in March 2020.

Executive Summary

The Deloitte Cyber Maturity Assessment shows that good progress has been across the 17 capabilities assessed. A high-level set of actions will be released and the full report is to follow.

We have been tracking statistics surrounding email-based attacks and user behaviour during the COVID-19 period. The results of this and follow on actions are included.

Questions addressed

1. What are the results of the Deloitte Cyber Maturity Assessment?
2. What is the impact of COVID-19 on email attacks and user behaviour?

Confidential

POL00423570

Report – Cyber Security Maturity Assessment

3. In March 2019 Internal Audit and Deloitte performed an assessment of POL's cyber security maturity using their Cyber Security Framework model and toolkit. The assessment measured the maturity of POL against 34 Cyber capabilities and calculated the gap between those scores and an agreed target maturity based on retail and FS benchmarks. Since that assessment, a coherent programme of work has been underway to close the maturity gaps and move POL towards the agreed target maturity values. Progress on this programme has been reported to the RCC and ARC at each meeting since.

4. In April 2020 Deloitte were re-engaged to assist Internal Audit in checking our progress against 17 of the 34 capabilities. The 17 were selected based on risk and importance to POL based on the current business environment.

5. We have internally tracked progress on all capabilities using our own measurement method which has previously been reported at this forum.

6. Deloitte will issue a full report containing detailed actions for POL to further mature Cyber controls later in July 2020.

7. In the interim, Internal Audit have worked with Deloitte to provide an overarching report giving key recommendations and maturity assessments provided. This report is available in the reading room with key results shown in Appendix 1.

8. In summary the results show that:

    a. We have notable strengths in cyber security and some areas to continue focusing on.

    b. 12 cyber capabilities have increased in maturity, some significantly in the areas connected with security monitoring, vulnerabilities, threat intelligence and data security.

    c. 3 capabilities have stayed at the same maturity levels since the last review namely cloud security, privileged user access control, and security platform administration.

    d. 2 capabilities have decreased in maturity, namely strategy & operating model and policies, standards, and architecture

9. Whilst most areas have increased in maturity the key question is - are we any less secure because of the areas that have stayed the same or reduced?

    a. Of the 3 capabilities that have stayed the same privileged user access control is already at target maturity. Cloud security has stayed the same as we are mid-way through changing our cloud security strategy to be based more around AWS. Security platform administration has stayed the same as we have

POL00423570



genuinely not changed how we are running our platforms. All these three have relatively high maturity scores (e.g. 2.xx) and would not adversely affect our security position.

b. For the 2 that have reduced the rationale is similar. Cyber strategies require an agreed business and corresponding IT strategy to provide context and help define strategic outcomes. As both are currently under development within POL then development of a 3-5-year cyber strategy was not sensible in 2019/20 and this was replaced by tactical rolling one-year plan. Also, Security architecture exists to support the cyber strategy which again explains why the score has reduced slightly in this area

c. During the last 12 months we have focused on enhancing the operating model, putting in place a fit for purpose cyber team and CISO. Deloitte have assessed and marked this appropriately.

d. In answer to the question posed at the start of this section is that we are overall more secure than we were a year ago but in the next year we need to focus on developing a strategy as the business and IT strategies unfold. This will have a further knock-on effect on maturity scores in other areas.

Confidential

POL00423570

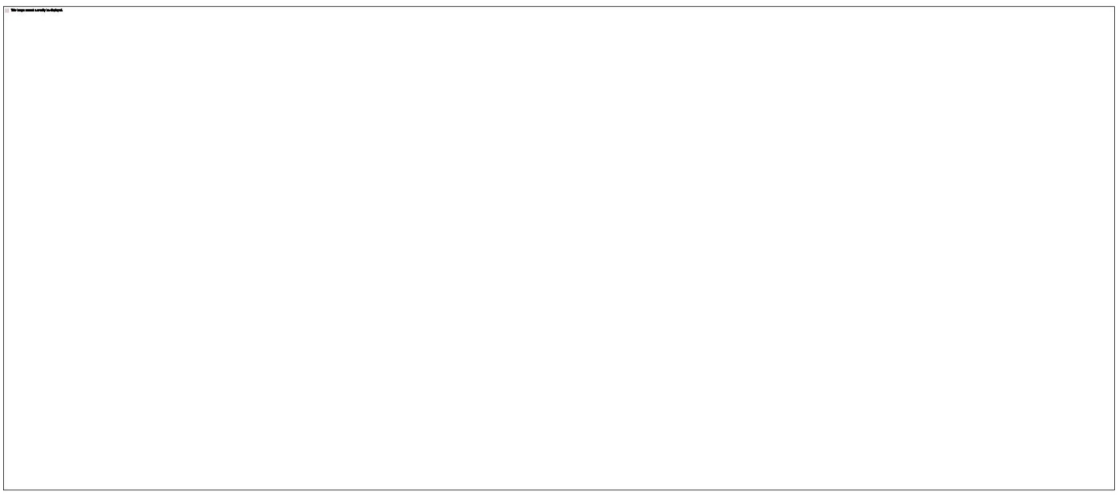
Report - COVID-19 Email & User behaviour

4

10. In the previous report to this committee we described the steps we have taken to keep POL secure throughout the changes brought about by the COVID-19 pandemic.

11. We have been logging and monitoring some key metrics since January which illustrate the changes during the COVID19 period.

12. The graph below shows the status regarding phishing attacks on Post Office:



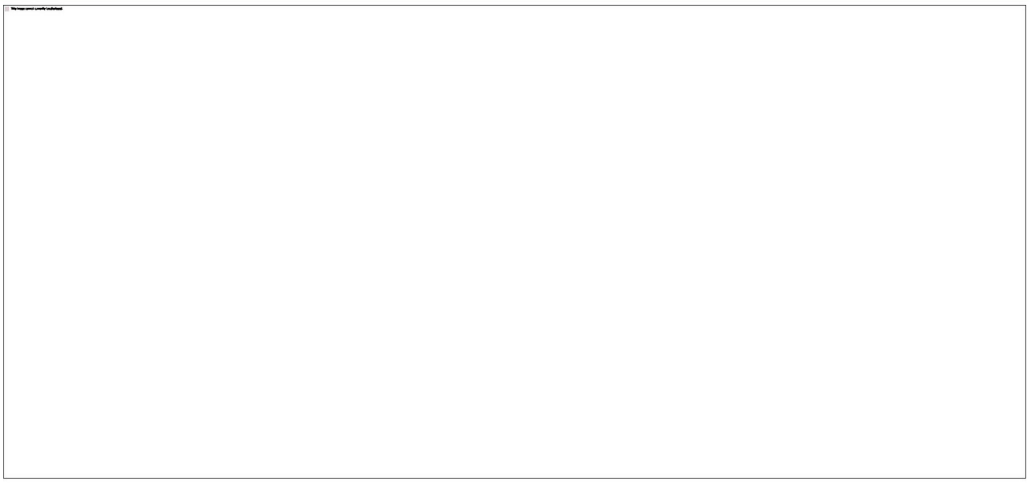
13. Phishing has risen and is continuing to rise as a method of attacking organisations.

14. Our phishing defences continue to work well but we need to stay focused. We have already run a targeted phishing simulation to raise awareness and will be targeting further activity in this area going forward – I am being vague here to keep the element of surprise!

15. The second graph below shows the spike in SPAM-based mail attacks over the COVID-19 initial period which now appear to have returned to normal levels.

Confidential

POL00423570



16. Finally, the following graph shows how user behaviour around sending emails to personal addresses with attachments has changed. During March to June, after COVID hit, there was disruption to people's working patterns and new policies in place regarding home printing. People were developing new ways of working at home which is why we have the large variation in values during this time.

17. Levels have now stabilised. We continue to contact those who break policy in this way to gently remind them of their responsibilities during this challenging time. T

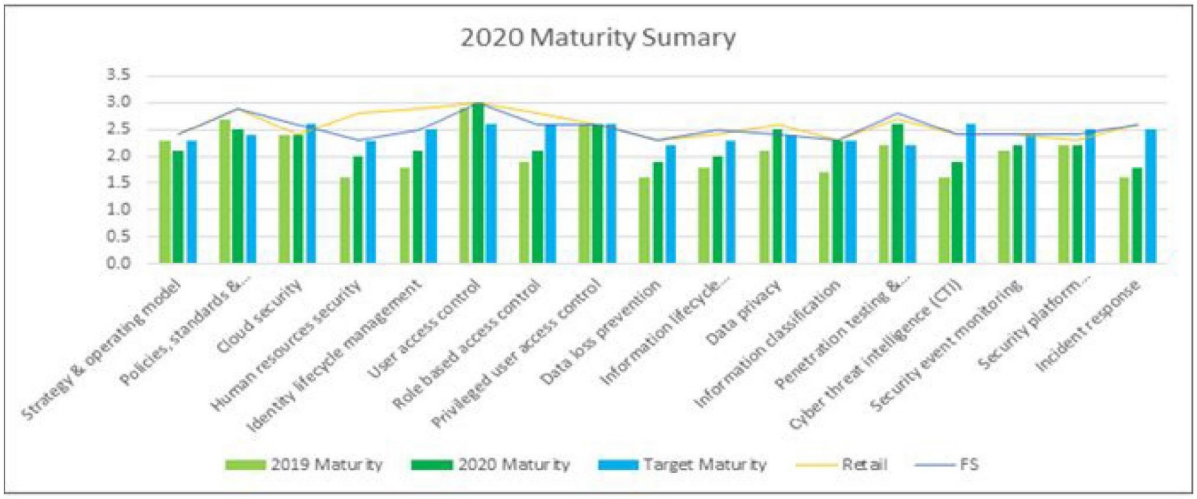


18. The residual percentage is quite high at 12%. This is due to a population of users within POL who need to send emails to personal addresses for business reasons e.g., some of those in branches. Our phase 2 DLP programme will provide the capability to identify these users allowing us to focus on the remainder.

Confidential

POL00423570

Appendix 1 – Cyber Security Maturity Assessment



Overarching Actions

A number of overarching actions have been agreed which reflect themes identified during the review and work needed to define target maturity and track actions. Detailed recommendations for each capability will be included in Deloitte's full report. Internal Audit will track progress against these 8 actions.

	Action	Rating*	Action Owner	Date
Scope Area: Governance				
1	Review and agree target maturity levels, reflecting any change in POL's risk profile.	P1	Tony Jowett	30 Sep 2020
2	Agree the list of Crown Jewels with POL's GE.	P2	Tony Jowett	30 Sep 2020
3	Document the cyber strategy in line with the business and IT strategies.	P1	Tony Jowett	31 Dec 2020
4	Document POL's current security architecture and patterns to support POL going forward.	P1	Dave King	31 Dec 2020
5	Develop an end-to-end cyber programme.	P2	Tony Jowett	31 Mar 2021
6	Update the cyber action tracker to reflect the detailed Deloitte findings and recommendations from the Cyber Maturity Assessment.	P1	Tony Hogg	30 Sep 2020
Scope Area: Secure				
7	Document and unify Joiners, Movers, Leavers processes as part of the JML project.	P2	Tony Jowett	31 Mar 2021
8	Develop and document a comprehensive Cloud security strategy, linking into the IT and cyber strategies.	P2	Adam Malach	31 Dec 2020

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

Confidential

POL00423570

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE

4

Title:	JML Update	**Meeting Date:**	13 July 2020
Author:	Tony Jowett, Chief Information Security Officer	**Sponsor:**	Jeff Smyth, Interim Group CIO

Input Sought: Noting

- To note the status and plans regarding the reduction of risk associated with Joiners, Movers and Leavers (JML)

Previous Governance Oversight

- Actions to report on this occurred at the previous Risk and Compliance Committee (RCC) in March 2020.

Executive Summary

Joiners, movers, and leavers continues to be a focus area with relevant findings in this area to come from the Deloitte review mentioned above. Key activities and next actions are included.

Questions addressed

1. What is the status and plans surrounding Joiners, Movers and Leavers?

Confidential

POL00423570



Report – Joiners, Movers and Leavers (JML)

2. We have divided JML into the following areas of focus:
    a. Colleague and contractor JML with standard access
    b. Colleague and contractor JML for privileged access
    c. Third party access to physical locations
    d. Third party running JML on their own systems on behalf of POL
    e. Underpinning technical infrastructure
    f. Automation and centralisation

3. Our efforts to improve ***colleague and contractor JML with standard access*** have focused around a project to enhance the integrity of the links between our HR system of reference Success Factors, Microsoft Identity Manager and Active Directory which controls access across the administration estate. This project is in flight and is expected to complete in August 2020.

4. In addition to this work there are several systems that we have anecdotal evidence are not being updated correctly – further investigation is required in Q2 to establish which ones are missing.

5. For ***colleague and contractor JML with privileged access*** there were 3 recommendations in the PWC financial audit two of which were against Horizon and one against Credence. One of these is closed with an effective control in place. The other two are being investigated further to understand what the next actions are.

6. For ***third party access to physical locations*** we have paused any activity in this area due to COVID-19.

7. We have examined more closely our arrangements for ***Third party running JML on their own systems on behalf of POL.*** The Cyber Security team run quarterly Information Security Management Fora to discuss issues and monitor remediations with our main tower vendors. The table in Appendix 1 shows the summary status of the tower vendors regarding JML and Privileged Access Management (PAM).

8. In short, we are currently relying on an attestation alone approach. Best practice is to supplement this with periodic spot audits to keep suppliers honest. Therefore, our next steps are to investigate how we would achieve this under the current contractual arrangements and resourcing.

9. At this stage we do not think it is sensible for us to manage JML on behalf of suppliers under current arrangements. However, the move to cloud (such as that in progress for the Belfast Exit project) presents opportunities for us to have greater oversight and control over JML in the future.

Confidential

POL00423570

10. On ***underpinning technical infrastructure***, the Deloitte Maturity assessment report will make detailed recommendations around the following capabilities that support JML:
    a. Identity Lifecycle Management
    b. Role Based Access Control
    c. Privileged Access Control
    d. User Access Control

11. Regarding ***automation and centralisation,*** we have developed a draft JML Reference model which aims to show the steps required for successful JML and the role of each POL department in it. The aim is then to use this model to align JML across the Post Office and to pave the way for greater use of automation.

12. We are considering options for our Identity Management operating model. One of the reasons that JML is difficult to improve within Post Office is that responsibility for it is spread across a range of different departments and organisations, each with their own objectives. JML resides with specific individuals who in some cases are single points of failure. A centralised access management function would be in line with best practice and would address these points.

13. The Deloitte Cyber Maturity report recommends the use of automation as far as possible. An automated Identity platform would have benefits in productivity, error reduction and audit readiness but would require investment. Once the detailed Deloitte recommendations and corresponding plans have been developed then this will be validated further.

14. We need to develop a range of metrics that point to any issues in the integrity of the end to end process – this is a target for Q2 2020.

15. The table below summarises the actions for Q2 2020

Area	**Action**
Colleague and contractor JML with standard access	• Complete the MIM Project • Identify systems missing from MIM
Colleague and contractor JML for privileged access	• Complete PWC audit actions
Third party running JML on their own systems on behalf of POL	• Add audit regime in line with contracts
Underpinning technical infrastructure	• Develop and action plans against Deloitte Cyber Maturity report
Automation and Centralisation	• Agree and publish JML reference model • Develop options for organisation • Validate requirements for automation
Metrics	• Develop a range of metrics to identify issues in JML

POL00423570

Appendix 1 – Tower vendor JML & PAM status

Vendor	Monthly JML Data	PAM Data
Atos	Provide monthly data on helpdesk staff – Current Staff List and Clearance level.	Not applicable
Accenture	Basic JML Data Provided Monthly, this included clearance and awareness training figures	Quarterly
Computacenter	Basic JML Data Provided Monthly, this included clearance and awareness training figures	Quarterly
Fujitsu Services	Comprehensive list provided monthly.	Monthly
Fujitsu Telecom	Basic data on privileged and user access accounts	As per monthly data.
Verizon	Provide Privileged Management Data on Post Office side. The Verizon staff audits covered separately Verizon staff	Discussed previously at ISMF , this was limited that providing this data provided limited value(it related to Verizon staff not visible to POL) - The JML checks (security clearance an training) are covered by the teams own ISMS and audited several times.

Confidential

POL00423570

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE

Title:	Business Continuity and Resilience Update	**Meeting Date:**	13 July 2020
Author:	Tim Armit, Business Continuity	**Sponsor:**	Jeff Smyth, Interim Group CIO

5

Input Sought: Noting and Policy Sign Off

- Report at request of the committee
- Business Continuity Policy requires annual sign off

Executive Summary

Business continuity solutions and levels of resilience have enabled the strong Covid19 response.

Third parties, stakeholders and external organisations have all asked Post Office for business continuity advice across the Covid19 period.

Home working has offered a potential new approach to administration buildings recovery strategy.

Crisis response and communication has been proven to be effective.

Consideration for a Covid19 second wave are now having war games discussed to stress test preparedness.

The business response to a complete Horizon failure remains the key risk.

The Business Continuity Policy requires annual signing.

Questions addressed

1. Do current levels of resilience and continuity plans in place meet Post Office requirements?
2. Are there key business continuity risks the Post Office is exposed to?
3. Annual sign off of the Business Continuity Policy is required

Confidential

POL00423570

Report

4. Do current levels of resilience and continuity plans in place meet POL requirements?

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

Continuity plans were implemented in February 2020 in preparation for the increased impact of the Covid19 pandemic. When lockdown was implemented home working was in place and solutions to support branches and Supply Chain already implemented.

Physical relocation solutions for Chesterfield, Bristol, Bolton and London are in place with Sungard and these have all been tested and proven to work. However Covid19 has demonstrated that Post Office can run 100% of administration offices with home working for an unlimited period of time. The ability to maintain call centres with home working was successful leading to Post Office being able to support the third party POCA call centre who did not have the same level of response plans in place. Changing to this as an ongoing continuity solution is now being considered and explored.

IT, HR and Communications all had to adapt their plans in place to support the levels of home working required and implement Policy and communications tools to enable and support home working for all administration staff.

Incident response and escalation methods are in place for all levels of incident. A new sub team to respond to branch incidents has been stood up and proven which links into the Business Protection team (BPT). The IT incident response team and its links to the BPT are proven and known by all involved. For specific ongoing longer term crisis events such as GLO post trial response and Covid19 a sub set of the BPT has been stood up and worked as a Rapid Response Team (RRT).

The RRT for Covid19 was stood up in mid-February 2020 to implement the plans and strategies to ensure Post Office continued operations against a number of scenarios. These plans were in place when lockdown was announced and minimised the impact on operations.

Post Office has been recognised by Government and across the Finance system as being ahead of most in their response, planning and ability to smoothly continue operations ensuring that :

- Call centres remained operational
- Circa 9000 branches continued to trade
- POCA services were delivered to all customers
- Working daily with RMG parcel levels exceeded Christmas levels
- Banking services found new personal banking customers as many banks closed
- Supply Chain continued to deliver and return cash and stock as required
- Payzone remained operational across the period
- Specific support was given by individual Post Masters to vulnerable customers

The Post Office on Wheels implemented in December 2019 has been deployed in conjunction with temporary Post Masters and mobile Post Offices to support any branch closures in key areas and ensured if critical branches could not trade a solution could be put in place.

Daily reporting against key metrics, branch closures, employee absenteeism and call centre capability were delivered across the period and developed into operational dashboards.

POL00423570



Grapevine communications support, Sungard third party provider of recovery space and Post Office key IT suppliers all maintained service across the period and have proven recovery capabilities in place.

Post Office has had strong business continuity solutions in place for three years and this exceptional crisis event has again proven the plans in place work, the crisis response is well rehearsed and implemented and that Post Office can be confident it can respond to crisis events in a controlled manner to meet business needs.

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

Yes, there is no coordinated strategy for the large scale failure of the Horizon system; this risk was identified in late 2018 and work was completed across all products and business areas and remains as reported in previous RRC and ARC meetings.

Ongoing work with product teams and IT on alternative solutions continues. The key is to ensure the systems are fully resilient in design with automatic fail over and uninterrupted service. As more services are transferred from the traditional Belfast datacentres to the AWS cloud resilience and reliability will increase and the capability to restore systems during an interruption will be enhanced.

6. Business Continuity Policy requires annual sign off

Policy attached for annual review and sign off.

Stakeholder Implications

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

Next Steps & Timelines

8. Ensure lessons learnt from Covid19 enhance planning and are included in future projects to increase ongoing resilience.
9. Support working at home projects, NEO and other developments evolving from Covid19 to ensure resilience is in design.
10. Ensure key areas, GE, HR, Communications are continually trained and rehearsed against scenarios to keep a strong response capability in place.
11. Ensure plans for a second wave or partial lockdowns are in place
12. Focus on Horizon resilience levels and continue to develop alternative working practices.
13. Support IT in reviewing root cause analysis and ensuring operational mitigations continue to meet business needs.
14. Continue to escalate the Post Office on wheels solution.

POL00423570





[*GROUP POLICY*]

[*Business Continuity Management*]

Version – V2.6

Chief Executive Endorsement

"If there is a single event when business continuity is brought into sharp focus for a Board and its senior leaders then Covid-19 is that event. The criticality of having a clear business continuity strategy and plan was critical to the timely response that Post Office made during the pandemic. We were able to continue to serve Postmasters and ensure they were able to serve their customers and communities. This is why we must review and validate and invest in our plans regularly."

Nick Read, Chief Executive Officer, June 2020

POL00423570



contents

1 Overview 4
1.1 Introduction by the Policy Owner 4
1.2 Purpose 4
1.3 Core Principles 4
1.4 Business Continuity Objectives 5
1.5 Application 5
1.6 The Risk 5
1.7 Legislation 6
1.8 Industry Guidance 6
2 Risk Appetite and Minimum Control Standards 7
2.1 Risk Appetite 7
2.2 Policy Framework 8
2.3 Who must comply? 8
2.4 Minimum Control Standards 9
2.4.1 Threats 11
2.4.2 Approach 11
2.5 Implementation 12
2.5.1 Satisfying BCMS Requirements 12
3 Tools & Definitions 14
3.1 Tools 14
3.2 Definitions 14
4 Where to go for help 15
4.1 Additional Policies 15
4.2 How to raise a concern 15
4.3 Who to contact for more information 15
5 Governance 16
5.1 Governance Responsibilities 16
6 Control 17
6.1 Policy Version 17
6.2 Policy Approval 17

5

POL00423570

1.Overview

1.1. Introduction by the Policy Owner

The Business Continuity Manager has overall accountability to the Board of Directors for the design and implementation of controls to prevent or deter failures in normal operations. The Business Continuity Management Policy details the approach to implementing strategies and plans to minimise the impact to operations and restore operations in a time to meet business requirements. This approach ensures the risks to operations are known, the impact to operations of failure are understood and recovery priorities are based upon the tolerance to impact. The Policy is an agenda item for the Audit and Risk Committee and the Post Office board is updated as required.

1.2 Purpose

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

1.3 Core Principles

Post Office adopts the Business Continuity Institute's Good Practice Guidelines definition of business continuity as: "A holistic management process that identifies potential threats to an organisation, and the impacts to business operation those threats, if realised, might cause, and provides a framework for building organisational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value- creating activities."

This Policy is consistent with "ISO22301", which is the Business Continuity International Standard. The purpose is to define the Group's policy with regard to business continuity management that is appropriate to its aims and objectives. This includes a framework for:

- Setting business continuity objectives;
- Satisfying appropriate legal, regulatory and contractual requirements;
- Continual improvement of the Business Continuity Management System ('BCMS'); and
- Key controls in respect of business continuity.

This policy should also be read in conjunction with other Post Office resilience, health & safety, and physical security related policies and procedures.

POL00423570

The following areas of Post Office's business are within the scope of the policy:

- All customer support centres including but not limited to, Finsbury Dials, Chesterfield and Bolton office
- All Supply Chain Locations
- All Directly Managed Branches
- All other Post Office Operational centres
- All external/outsourced Supply Chain Capability.

Out of Scope of this Policy:

- All IT systems – these are covered within the Information Disaster Recovery Policy

This policy's effective date will be determined by the date on which final approval is given by the appropriate governance forum

1.4 Business Continuity Objectives

Based on the requirements and factors set out in this document, the following major objectives are set for business continuity:

- Objective 1 - Comply with health and safety legislation at all times
- Objective 2 – Maintain stakeholder confidence
- Objective 3 – Maintain customer service levels
- Objective 4 – Minimise loss of revenue

The success of the BCMS will be judged on its ability to meet these overall objectives.

1.5 Application

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

The Policy should be considered within Change and Procurement and onboarding of new services, suppliers or business units.

The Policy applies to all business units and operations and should ensure plans, strategies and requirements are known for all areas to minimise the impact of any interruption.

The risk to the Group from Business Continuity is reviewed by the board annually.

1.6 The Risk

The Business Continuity Policy is designed to help mitigate the risk that normal operations are interrupted and not restored in a controlled and timely manner with the consequence that:

- Staff and Customers safety is at risk;
- Customers are unable to be served;
- Regulatory requirements are not met;
- Legal and contractual breaches occur;
- Income is affected; and
- Confidence in the Post Office's reputation is harmed.

POL00423570

1.7 Legislation

The Group is subject to a variety of legal and regulatory requirements which either apply directly or are imposed through contractual arrangements with key clients. These include, but are not limited to:

- Health and Safety legislation;
- Payment Card Industry – Data Security Standard compliance;
- Financial Services legislation;
- National and international standards e.g. ISO9001; ISO270001; and
- Consumer protection legislation.

1.8 Industry Guidance

ISO22301 is the accepted International Standard for Business Continuity. There are other Standards on Operational Risk, Information Security, Crisis Management and IT Disaster Recovery.

The Business Continuity Institute issues good practice guidelines The FCA

issues best practice guidelines

POL00423570

2 Risk Appetite and Minimum Control Standards

2.2 Risk Appetite

- The following risk appetite statements are relevant to Business Continuity:

  Averse appetite for taking risks which might result in failure to maintain the service commitment in respect of customers in line with our social purpose and Government's policy on subsidy**.**

  Neutral risk appetite for dissatisfaction related to BAU services recognising that in a complex business there will be a level of dissatisfaction as part of the normal course of business of achieving our commercial objectives.

  Averse appetite for risk taking which would alienate or lose significant groups of profitable customers

  Tolerant risk appetite for customer dissatisfaction caused by transformation, innovation and customer selection/profitability decisions.

  Neutral appetite for risk taking which would have a detrimental impact on vulnerable customers. Post Office will take a balanced view, reflecting commercial implications of introducing safeguards and controls to protect vulnerable customers and the needs of those customers.

- Post Office takes its legal and regulatory responsibilities seriously and consequently has:

  Tolerant risk appetite for Legal and Regulatory risk in those limited circumstances where there are significant conflicting imperatives between conformance and commercial practicality

  Averse risk appetite for not complying with law and regulations or deviation from business' conduct standards

  Averse risk appetite for unethical behavior including staff misfeasance, failure of, governance and control processes, critical financial reporting processes, and critical supply chain and business continuity processes.

- Post Office is committed to safeguarding the wellbeing of its people and therefore has:

  Averse risk appetite associated to the health, safety and wellbeing of POL customers and colleagues in everything we do. This is paramount to every aspect of POL operation. This includes; loss of life, serious injury and non- compliance to regulation and policy

5

POL00423570

Post Office is committed to exploiting technological benefits to achieve market advantage. In recognition of this, Post Office has:

> ***Averse*** appetite for data loss/leakage that can lead to customer, commercial or reputational damage
>
> ***Neutral*** appetite for operational IT services
>
> ***Averse*** risk appetite for any serious impact to the confidentiality, integrity and availability of information, leading to financial loss, business disruption, public embarrassment or legal consequences.

Post Office recognises that it cannot completely eliminate business continuity risks. However, this policy sets out controls to reduce and/ or mitigate such risks.

This level of risk appetite will be applied to the risk assessments that are carried out as part of the BCMS and will determine the actions that need to be taken to mitigate risk to an acceptable degree.

2.3 Policy Framework

Post Office has established a suite of resilience and risk policies, on a risk sensitive approach which are subject to regular review. Other policies which may be relevant to business continuity include the following:

- IT Disaster Recovery
- Information Security
- Data protection

2.4 Who must comply?

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

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

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

POL00423570

2.5 Minimum Control Standards

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

The table below sets out the relationships between identified risk and the required minimum control standards in consideration of the stated risk appetite:

Risk Area	Description of Risk	Preventative Controls	Corrective Controls	Who is responsible	When
All	BCMS is not fit for purpose. May lead to inadequate strategies and plans being implemented that do not meet business needs.	Annual review of the BCMS content and effectiveness. Internal Audit review	Updated on change of approach or discovery of gaps.	Business Continuity Manager Audit Manager	Annually
All	Risks the business and locations are exposed to are not known or are inadequately mitigated.	ISO22301 defines managing Business Continuity risks to include an assessment of : • Threats; • Vulnerabilities; • Impact & likelihood before risk treatment; • Risk treatment (e.g. reduction, removal, transfer); • Function responsible/ owner; and • Timescale and review frequency.	As risks are identified or occur and root cause analysis is completed risks and threats are added to the assessment matrix to ensure business areas continually challenge their strategies against new risks.	Business Continuity Manager. Risk Manager IT DR Manager. Facilities Manager. Location PICS. Business Leads.	Annually

POL00423570

Risk Area	Description of Risk	Preventative Controls	Corrective Controls	Who is responsible	When
All	The impact on operations of a business continuity incident is not clearly understood.	Impact is measured against agreed metrics and agreed times to ensure business areas can be compared and strategies implemented which are compatible with the risk and impact the operational area is exposed to.	Impacts are challenged and after any incident or exercise reviewed to ensure the assumed impact meets the actual impact observed.	Business Continuity Manager. Business Leads	Every two years or on change.
All	Recovery strategies do not meet business needs	Annual tests of strategies in place to ensure business has confidence and understanding in the capability	Strategies updated after tests or actual incidents to ensure they meet business needs.	Business Continuity Manager All business leads	Annually
All	Contingency plans are not in place or available.	Plans in place must be assessed by internal audit and annually the status presented to the RCC. Plans must be held by all managers and available in a single accessible repository.	Plans updated after tests or actual incidents to ensure they meet business needs.	All business leads Business Continuity Manager	Annually
Business Protection Team (BPT)	BPT does not know the process to respond to a crisis	All BPT members are contacted and involved in crisis conference calls and undergo training.	BPT lists reviewed regularly and updated on change of roles or personnel.	Business Continuity Manager BPT members	Twice yearly
All	Staff are unaware of how to respond to a crisis	All staff are briefed and made aware of their responsibilities	Standard communications tools to brief staff, staff involved in testing, managers required to challenge their own plans and update them.	Business Continuity Manager All business leads	Ongoing
Building unavailable	Any key operational site may become unavailable for its purpose.	Risk assessments of sites are carried out annually by CBRE and POL. Strategies for the recovery of key operations per site are in place and annually tested.	Facilities and CBRE review risks regularly and provide options to enhance resilience levels to management.	Business Lead. Facilities Manager. Business Continuity Manager.	Annually. Upon moving in.

POL00423570

Risk Area	Description of Risk	Preventative Controls	Corrective Controls	Who is responsible	When
IT system failure	Any IT system can fail at any time.	This is managed under the IT DR policy and the IT COBIT process. All systems are documented and the impact of them failing documented. Resilient and DR capability is in place and managed by IT. This is tested annually.	Managed within the ITSCM role and covered in the Disaster Recovery Policy	CIO IT DR lead Business Leads Business Continuity Manager	Annually Upon Change. Upon impleme-ntation
Supply Chain distribution failures	Depots, Vans and operations may fail leading to routes and deliveries and collections not meeting business needs.	Plans and strategies to mitigate failures are in place and tested. Contingency planning for the loss of all forms of assets are tested.	Strategies updated after tests or actual incidents to ensure they meet Supply Chain needs.	Supply Chain lead Depot Leads Business Continuity Manager	Annually
Outsourced or supplier failure	Post Office relies heavily on suppliers and outsourcing to achieve its day to day operations. Any of these could fail or go out of business.	Part of the contract allocation and contract management covers business continuity. All suppliers commit to meet business continuity requirements and to test these. Contracts must contain appropriate BC and DR capability statements. Suppliers should demonstrate their recovery capability before a contract is signed, on review of the contract and if necessarily post any incident that affects them. Capability to restore operations in stated timeframes must be tested annually by all key suppliers. Suppliers to be categorised according to the risk their failure presents to Post Office. Many key suppliers will be within IT and the business consequence of an IT supplier failing must be shown to be mitigated by IT DR tests within these suppliers.	Contracts challenged if gaps are found, suppliers required to demonstrate their capability and contracts reviewed if gaps identified. Business areas required to implement plans to cover gaps in suppliers recovery capability.	Contract owner. Area dependent on contract. Business Continuity Manager. IT DR manager	Annually

POL00423570

Risk Area	Description of Risk	Preventative Controls	Corrective Controls	Who is responsible	When
Staff unavailable	Post Office staff are key to the success of day to day operations. At any time due to weather, health or any scenario staff may be unable to work.	Identification of single point of failure staff is undertaken within the contingency planning.	Key roles must be documented and where possible dual role training undertaken. As a working example the dependency on skilled drivers is key to supply chain and this is mitigated by the Rapid Response Team when required.	All business leads HR leads Business Continuity Manager	Ongoing

POL00423570

2.5.1 Threats

Post Office plans for the worst case scenario and does not work to specific threats unless they are beyond the scope of the risks planned for. Threats continue to vary and these will be used to define scenarios for exercises. Threats include:

- Weather related events
- Infrastructure failure
- Pandemic
- Cybercrime
- Environmental disasters
- Terrorism
- Industrial Action

2.5.2 Approach

In the approach to implementing, managing and reviewing business continuity capability the Post Office will:

- Create a Business Continuity Management System in line with ISO Standards showing the detailed approach to implementing and managing business continuity;
- Complete Risk and Impact assessments of tangible and intangible losses. To include an understanding of contractual and regulatory obligations, potential causes of risks, and impact of events both in terms of direct financial loss, cash flow interruption, customer impact, operational consequences, reputational impact and legal/regulatory impact. These assessments allow prioritisation of time and resource to implement recovery solutions;
- Develop and document strategies and plans to address key risks;
- Implement plans and recovery strategies (eg resilient IT, offsite recovery locations etc);
- Manage the central and local storage of plans;
- Annually (or more frequently) review plans;
- Consider impact of change activity on plans as part of major change activity;
- Create, manage and facilitate Post Office crisis response;
- Report all incidents and their impact;
- Test all strategies to ensure they meet business requirements;
- Integrate with IT recovery capability to ensure it meets business requirements;
- Train staff in the contingency plans and their roles and responsibilities;
- Complete root cause analysis when there is a (material) incident and review the control framework to include 'lessons learned';
- Embed appropriate and proportionate contractual requirements in contracts with suppliers and outsourcers including reporting, audit and rectification rights;
- Ensure there is regular oversight/testing of supplier and outsourcer obligations;

POL00423570

2.6 Implementation

The approach to implement business continuity within Post Office are defined within this Policy. These are the fundamental steps required which are led by business areas, facilitated by the Business Continuity Manager and are not subject to frequent change. The Post Office GE will ensure that adequate funding is available for activities identified in the implementation and ongoing support of the business continuity process.

Amendments to the Business Continuity objectives will be managed through the standard Post Office change management process if required.

2.6.1 Satisfying BCMS Requirements

Senior Managers commit to the provision of the appropriate resources to establish and maintain the BCMS and its outputs.

Regular review of the BCMS. This is conducted by the Business Continuity Manager on an annual basis, ensuring that objectives are being met. Evaluation of the current capability is undertaken and any issues identified through this audit programme and management processes are reported to the RCC. Management review includes departmental and other management meetings and document review.

Role definition and responsibilities are defined in the BCMS and reviewed by the Business Continuity Manager to ensure that colleagues understand the roles they are required to fulfil, and that they have the appropriate skills and competences to do so. These controls are necessary to ensure the continued BCMP success and to mitigate risk. Training will be provided where gaps in competency are identified and regular reviews of staff capability will be undertaken within departmental exercises.

Use of third parties. Post Office uses third parties, both internal and external, in the delivery of products and services. The ability to continue to provide these services or restore them should a supplier fail is key to Post Office operations and part of all contracts. This supplier capability will be evidenced by documentation and records, including contracts, meeting minutes and IT DR and BC test reports.

Continual improvement:

To ensure the approach to implementing and managing the BCMS is enhanced in an ongoing manner Post Office will:

- Consider effectiveness of the BCMS across all business areas and end to end systems, processes within scope;
- Enhance current processes to bring them in to line with best practice (as defined within ISO 22301);
- Increase the level of proactive continuity planning across Post Office;

POL00423570

- Achieve an enhanced understanding of and relationship with the business units to which the BCMS applies;
- Review relevant metrics (impacts, risk etc) on an annual basis to assess their appropriateness, or to make changes to them based on collected historical data and feedback or in response to incidents;
- Obtain ideas for improvement via regular review meetings with stakeholders.

Ideas for improvement may be obtained from any source, including but not restricted to: Customers; Suppliers; Colleagues; Risk Assessments & Audits.

In order to evaluate any proposed improvements to the BCMP, the following criteria would be applied:

- Cost;
- Business benefit;
- Risk;
- Implementation timescale; and
- Resource requirement.

Accepted improvement proposals will be prioritised, and planned according to standard project management principals.

POL00423570

3 Tools & Definitions

3.2 Tools

None in place

3.3 Definitions

Term or Acronym	Description
BCMS	Business Continuity Management System, the set of controls in line with ISO22301 to implement and manage business continuity
BC	Business Continuity
ITDR	IT Disaster Recovery, the recovery of IT systems and data
ISO 22301	The International Standard for Societal Security (Business Continuity).

POL00423570

4 Where to go for help

4.2 Additional Policies

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

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

4.3 How to raise a concern

Any Post Office employee who has concerns about a failure to comply with this policy has a duty to:

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

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

4.4 Who to contact for more information

If you need further information about this policy or wish to report an issue in relation to this policy, please contact Tim Armit – Business Continuity Manager by email at **tim.armit** GRO

POL00423570

5 Governance

5.1 Governance Responsibilities

Post Office's Board of Directors have overall responsibility for ensuring that Post Office has a framework to ensure compliance with legal, regulatory and contractual requirements. The Board is kept abreast of relevant matters relating to the management of business continuity by reports from its committees including its ARC Committee. The key individuals and their specific responsibilities in relation to this policy are:

- The Chief Information Security Officer (CISO) isthe Group Executive Owner and Policy Sponsor, accountable to the Board.
- The Group Business Continuity Manager is the Policy Owner who is responsible for:
    - Day to day implementation of and compliance with this policy and is accountable in this regard to the CISO;
    - Ensuring that there is an annual review of this Policy and tests compliance across the Group.
    - Providing appropriate and timely reporting to the Risk and Compliance Committee and the Audit and Risk Committee.

Post Office's internal systems of business continuity risk control ensure that controls are regularly independently assessed for effectiveness, suitability and adequacy. In addition, Internal Audit will periodically test compliance with this policy.

POL00423570

6 Control

6.1 Policy Version

Date	Version	Updated by	Change Details
19th May 2016	1.0	Jon Waples	First signed version
25th Feb 2018	2.0	Tim Armit	For review and signature
8th March 2018	2.2	Tim Armit	Typo changes
26th May 2020	2.3-2.6	Tim Armit	Annual review and signature, updated CEO statement

6.2 Policy Approval

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

Committee	Date Approved
POL R&CC	13th March 2018
POMS R&CC	27th March 2018
POL ARC	
POMS ARC	

Policy Sponsor: **Chief Information Security Officer**

Policy Owner: Business Continuity Manager

Policy Author: Business Continuity Manager

Next review: *date of next review 01 03 2021*

Company Details

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

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

POL00423570

Information Commissioners Office registration number is ZA090585.

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

7 Glossary of terms

7.1 Key terms and acronyms used

Business Protection Team Known as the BPT. This is the first response crisis teams to all significant events across the Post Office. It works as the Post Office Silver Team providing tactical response to significant incidents. It reports to the Gold Team which is the GE who provide strategic support and manages the Bronze teams to provide operational response to the issues.
Business continuity measuring impact and risks to the operations across the business and implementing strategies and plans, which are tested, to mitigate and minimize the impact and ensure timely recovery of operations.

POL00423570

POST OFFICE LIMITED RISK AND COMPLIANCE COMMITTEE REPORT

Title:	GDPR Contract Remediation	**Meeting Date:**	13 July 2020
Author:	Jonathan Hill	**Sponsor:**	Ben Foat: General Counsel

Input Sought: Noting and Approval

Previous Governance Oversight: Not applicable

6

Executive Summary

1. This paper reports on the outcomes of the new GDPR Contract Remediation project, which took place between December 2019 and the end of June 2020.
2. Under the original GDPR programme, the contract workstream involved (i) the amendment of all supplier and client contracts across the Post Office to include the relevant contractual clauses required by GDPR, and (ii) execution by supplier or client of all amended contracts. At the time the programme was shut down, not all contract amendments had been sent out to or agreed by the relevant supplier/client.
3. Progress was made throughout 2018, but further activity ceased when the GDPR programme ended in April 2019.
4. A new project was approved in November 2019 to close out the contracts that had not been remediated during the original programme. The project was given a £250K budget and was tasked to complete its work by end June 2020. Estimated spend at completion is £118K.
    a. 243 contracts needing to be remediated were identified initially
    b. 242 additional contracts, which had been de-scoped during the original GDPR programme were brought back into the project as the de-scoping rationale had not been recorded
5. The new project objectives:
    a. To remediate the outstanding 243 contracts
    b. To review the de-scoped 242 contracts to determine if they should remain de-scoped or be remediated

The Committee is asked to:

6. Note the report, and
7. Approve the approach to remediation activity going forward

Confidential

POL00423570

Project approach

8. Initially, 243 contracts had been identified as still needing remediation. However, no records could be found as to why a further 242 contracts had been de-scoped from the original GDPR programme.
9. In order to ensure GDPR compliance, these additional 242 contracts were brought into the new project until the rationale for de-scoping could be identified and approved.
10. The project was led by Compliance and supported by Legal, with a small project team. All contract remediation activity closure was approved by the Post Office Legal Director, Compliance Director and the DPO.
11. Contracts were prioritised depending on their materiality to Post Office and the GDPR risk. If the counter-party would not engage with Post Office and the contract was deemed to be low risk, then a "Deemed Consent" approach was taken, as approved by the ARC in November 2019.
    a. Deemed consent will not remove the legal risk but is a pragmatic approach to close out the remediation work.
    b. Given the changes in the GDPR legislation and the concept of dual accountability the ICO will consider the efforts made by Post Office to remediate the contracts in line with legislation and the failure, by our contracting parties, to engage.
12. If a counter-party taken down the deemed consent route wished to enter into negotiations with Post Office we agreed with their request.

Project status

13. All 485 contracts have now been reviewed and actions taken (please see Table 1)
    a. 272 went through a remediation process and 213 that were originally de-scoped had their status confirmed.
14. Of the 272 that have gone through a remediation process, 22 were returned to the contract owners as other contractual activity with the counter-party was or is about to be underway. All of these will continue to be supported by the Compliance Data Protection Team and Legal as part of normal BAU activity.

    These agreements were returned to the business for various reasons:
    a. Contract was due for renewal could be picked up as part of that work
    b. Wider sensitive negotiations were ongoing with the counterparty
    c. Business were looking to amend the contract and it was decided that GDPR remediation could be picked up as part of the amendment
    d. Out of the 22 agreements, seven have been highlighted as high risk:
       - CWU
       - Unite
       - Fujistu Telecoms

Confidential

POL00423570

- Global Payments
- OH Assist
- RAPP
- Selenity

e. All are being addressed and have support from the Legal team and/or the Data Protection team

f. Caseworkers from Legal and Compliance will continue to work with the contract owners to see these through to completion.

Table 1

Contracts in Remediation (as at 26.06.2020)	
Contracts identified for remediation	243
Re-scoped contracts returned to remediation	29
Total	**272**

Remediation completed / de-scoped	**237**

• *Remediated*
  ○ *Re-negotiated*
  ○ *Completed through deemed consent*
	48
	27
	21

• *De-scoped following review*
  ○ *Already remediated*
  ○ *Contract to be terminated*
  ○ *Duplicate contract*
  ○ *Licence agreements (no GDPR impact)*
  ○ *No evidence of live contract*
  ○ *No personal data being processed*
  ○ *No longer has POL relationship*
  ○ *GDPR policy under pre-existing agreement*
	189
	26
	4
	16
	102
	
	8
	21
	11
	1

Contracts moved to BAU for remediation	**22**

Contracts still in remediation	**13**

Closing out contracts still in remediation

15. Table 2 sets out the current status of the 13 contracts still going through remediation.

Table 2

Contract	Status	Next Steps
Verizon UK Ltd	Verizon and POL do not agree on Verizon to flow down terms to its sub-processors and 3rd party rights	Meetings happening w/c 29.06.20 to resolve
Inchcape	Inchcape and POL do not agree on data relationship but resolution now close. Our external lawyers are reviewing the Inchcape mark-up and will provide comments to Inchcape w/c 29.06.20	Agreement looks close but a further meeting may be needed to address any further issues arising from the mark-up
BT (bill payment)	Lack of engagement from BT following feedback from POL.	Meeting scheduled with BT for 30.06.20. BT now keen to close out

POL00423570

Santander (bill payment)	Lack of engagement from Santander. Now re-engaged with a proposal from Santander to follow Payout terms	POL agrees in principle with proposal. Expectation that close out should follow shortly
SSE Electricity (bill payment)	Internal SSE governance issue following OVO acquisition of SSE bill payment business needing novation.	GDPR terms agreed and contract should be executed once internal SSE issues closed [ETA mid-July]
Experian	No engagement from Experian. Experian claiming Covid-19 issues but also dispute on letters Experian claim sent in 2018	Have escalated to Julie Thomas
Fujitsu	GDPR discussions frustrated by wider contract discussions. FJ is resisting changes and has proposed a reduced liability cap. It has been escalated to POL CIO	Internal approach meeting with POL Fujitsu team scheduled for 30.06.20 To agree how to fit this in with wider discussions
Government Digital Services (Cabinet Office)	GDS contract runs until September 2021 as part of framework agreement. Changes were made in 2018 by GDS to bring into line with GDPR. As part of new GDPR project we reviewed terms and identified issue about POL status as data controller. Liability issue if there is a data breach outside of POL control as cannot pass through to GDS.	Proposed that Risk is accepted onto Identity Services risk register until contract ends in 2021 as contract cannot be changed now
NCR	Lack of NCR engagement since mark-up sent to them. Expect anything outstanding can be quickly resolved	Escalated to contract owner to push for response. Expectation high of 30.06.20 closure
Charities Trust	This is a Deemed Consent approach. Deemed consent deadline expired on 27.06.20.	Will be sent to CoSec for noting as deadline expired
Scottish Widows	Lack of Scottish Widows engagement since variation agreement reviewed by POL and comments sent to them. Expect anything outstanding can be quickly resolved	Continue to chase for closure. Expectation high of 30.06.20 closure
Investments Discounts Online	POI contract – proposed by POI to wait until agreement renewal to change.	Going to POI Risk & Compliance Committee for approval on 30.06.20
Accenture (now Duck Creek)	POI contract – proposed by POI to de-scope	Going to POI Risk & Compliance Committee for approval on 30.06.20

16. It is proposed to continue closing out these contracts using resources from Legal and Compliance working alongside the contract owners. Project management resource has ended as it is been reassigned to other projects. The activity will continue to be tracked by Compliance. The Committee is asked to approve this approach.

Jonathan Hill

29th June 2020

POL00423570

POST OFFICE LIMITED
RCC Paper

Title:	Project Assurance – RM Pensions (POL Section)	**Meeting Date:**	RCC 13.07.2020 ARC 27.07.2020
Author(s):	Martin Letherbarrow Maxine Cross	**Sponsor(s):**	Al Cameron Lisa Cherry

Input Sought:

Noting that:

- work is in progress to quantify material errors uncovered in pensions data - and the related impacts/risks these errors present
- the options to resolve the errors and mitigate risk
- an internal audit has been commissioned to examine related processes/systems

Decision:

- The issues identified are potentially notifiable to The Pensions Regulator (TPR) and could give rise to civil penalties. At this point, however, having regard to the speed and extent of the remediation project, it is recommended that no report to TPR is made at this stage but that the question of whether a report should be made is kept under review. Does ARC support that recommendation?

7

Previous Governance Oversight

CR approved 26.3.2020 in relation to the investigations into, and correction of incorrect promotional increases to RMPP final salaries; and the knock on effect to the buyout project, extending the delivery timeline to Feb 2021.
Board paper 23.09.2019 to gain approval for the partial buyout of Defined Benefit pension liabilities related to the RMPP Post Office Section.

Executive Summary

In preparation for the partial buyout of the RMPP (POL section) pensions' liabilities, the project identified material systemic errors in the provision of pensionable data, by Post Office to Royal Mail Pensions Service Centre. These errors (overstating pensionable pay), are predominantly linked to the incorrect configuration of Success Factors, introduced in January 2018; and the misinterpretation of how promotional increases are treated.

Specialist resource (from Willis Towers Watson, our actuarial advisers) has been engaged to work with the project team to help identify the extent of these errors, and to assist in the mitigation of future error. An internal audit has also been commissioned to identify how the errors came about, why they were not spotted before and to ensure lessons are learnt for the future.

A deep dive is still in progress to quantify the errors (at an individual member level) and to assess the likely impact on pensions' liabilities and funding of the plan, but is anticipated that this will conclude in the next month or so. Our expectations are that when this phase is complete, focus will need to move quickly to:

- correct records for 'active' members who remain in Post Office employment and are not yet in receipt of their pensions. Incorrect pensionable pay figures may never have been communicated to these members

Confidential

POL00423570

- correct records for 'deferred' members who have left Post Office employment and are not yet in receipt of their pensions. Incorrect pensionable pay figures may have been communicated to these members when they left Post Office, so adjusted figures will need to be communicated
- work in partnership with the Trustee to consider what action is to be taken where members are found to be in receipt of incorrect pensions (or where transfer value payments have been made to other pension schemes). In law, it is clear that the Trustee must stop overpaying benefits as quickly as possible, and should be expected to recover most if not all of any overpayments to date (although there are value for money considerations). In practice, there are other important considerations to take into account before deciding how to address the overstated benefits – including reputational cost, member's hardship and appetite of Post Office to seek a more generous outcome for the affected members than is required by law (such as augmenting benefits the overstated level). The latter option is likely to have a significant direct cost implication to Post Office.

Questions addressed

1. What pensionable pay data issues are there? What went wrong and why?
2. What are the potential impacts on members?
3. What are the likely impacts on the actuarial valuation, 2017 buy-in and planned buy-out?
4. What are the legal risks from the pensionable pay transmission errors?

Report

What pensionable pay data issues are there? What went wrong and why?

Material errors have been discovered in the provision of pensionable data, by Post Office to Royal Mail Pensions Service Centre (RMPP PSC). These include:

- Double-counting of allowances data which has led to a potential £3m overstatement of pensionable pay figures transmitted to RMPP PSC and which feed into the calculation of pension benefits. Incorrect configuration (and absence of proper design and testing) of the Success Factors system introduced in 2018 is the likely point of failure.
- Data shows that in some cases a full promotional increase has been applied where the correct treatment, per the scheme rules and circumstance of the promotion, would have been to apply none or part of the increase. At this stage we do not know who is affected by this issue without re-doing calculations for every salary increase since 31 March 2014 – This is in progress.

A number of 'second order' and far less material anomalies have been identified, such as:

- erroneous application of annual RPI increases to allowances incorrectly incorporated into base pay for RMPP purposes
- the erroneous order of annual RPI increase routines and the comparison of simultaneous changes to pay, within these routines to scheme 'underpins'
- discretion applied to basic pensionable salary, which is not permissible per the scheme rules, in the case of 'step downs'

Our advisers have described the RMPP (POL section) rules as the most convoluted they have ever come across; and the lack of clarity and understanding of how these rules translate into administrative application is likely to have contributed to the issues we have found.

What are the potential impacts on members?

The effect on member benefits depends on whether a member is still employed (active), has left employment (deferred), retired or died. The table on page 4 of the attached appendix shows a breakdown of the two material issues and the split of member status as at 30 April 2020.

Financial Impact

Effect on actuarial valuation?

Although the triennial actuarial valuation was carried out in 2018, the allowances data was taken from the old admin system, so the double-counting issue should not affect the results of the actuarial valuation

Confidential

POL00423570

(and is also why the error wasn't identified at the time). There will be a limited impact from the pensionable pay increases issue for increases received between 31 March 2017 and 31 March 2018, and from the less material issues covered above.
To get some sense of scale of these issues in relation to increase in pensions' liabilities if no resolution were pursued. If we were to apply the ratio from the 2018 valuation report of pensions liabilities (£192m) to pensionable salary for actives (£54m) i.e. 3.55:1; then the potential £3m overstatement of allowance figures, in a very broad brush (and hugely caveated) translation would amount to £10.65m in potential pensions liabilities (£3m x 3.55). The actual figure is of course dependent on the profile of the affected members and their 'rebuilt' salary / benefit figures etc. so this high level assessment could change dramatically (up & down).

Effect on 2017 buy-in data?

There is nothing in our findings so far to indicate that there is a material issue with the buy-in data, because the material problems originated after the data extract for the buy-in was taken.

Effect on planned buy-out?

Progress on the original scope of the buyout project is dependent on appropriate resolution of the errors that are discovered. Current estimates are that the completion of the partial buyout will be pushed out to summer 2021. This timescale is still well within the 1 April 2022 deadline on which The Trustee has to make all buy-out requests on the current terms.

7

Risk Assessment, Mitigations & Legal Risks

Risk	Considerations/Mitigations	RAG
Possible Additional funding of RMPP Legal claims from affected members would almost certainly be against Trustees not POL. The cost of remediating the errors are likely to be paid from scheme surplus, not POL. Additional scheme funding liabilities to POL are only likely to arise if: - affected members were to claim successfully against the Trustee for benefits based on the higher, incorrect pay data, and/or a financial award for distress and inconvenience. - the right to recover overpayments were waived - POL were to augment members' benefits where no legal requirement exists.	There is a reasonably high risk of claims from disappointed members as it is cheap and easy to access the Pensions Ombudsman (TPO) complaints process. However, the chances of any individual member succeeding in a claim for windfall higher benefits appear slim. There is a significant surplus which will likely readily cover additional remediation, although it is possible that Trustees will seek contribution from POL, which remains to be seen. This will however need to be kept under review. Whether POL would agree to augment members benefit will be within POL's gift to be assessed once more is known about the extent of the liabilities, the cost and scope or remediation and reaction of beneficiaries. Again, to be kept under review.	
Breach of statutory duties and associated whistle-blowing/notification requirements POL has a statutory duty to provide accurate pay data to trustee. We may have breached that. The Trustee has its own duties, which it may also have breached. Breach of law is potentially notifiable to The Pension Regulator (TPR). POL the Trustees and their respective legal advisers have that duty.	There is extensive guidance around the test for whether a breach of law should be reported to the Pension Regulator. Applying that guidance, having regard to the speed and extent of the remediation project, it does not appear that the issues discovered to date would be reportable. However, is recommended that be kept continuously under review.	

POL00423570

The penalty for a breach of law is a civil penalty of up to £50,000 for POL. For Individual directors TPR could also apply a civil penalty of up to £5000 to a director or other officer of POL if the act or omission leading to the breach of duty was done with the consent or connivance of, or is attributable to any neglect on the part of, that person.	It is understood that neither the Trustees nor either party's legal adviser has taken the view that this is reportable at this time. If a fine was levied against individual directors or POL, it may be covered by POL or POL Directors' and Officers' insurance. Of course, whether any civil penalty is levied is covered by POL or D&O insurance, cannot protect against reputational risk, although that should be mitigated against by a frank open and cooperative approach with members and unions. POL and/or directors may wish to legal advice on this point before reaching a view about whether to report to TPR.	
Claim by the Trustee in negligence for damages for the Trustee's own rectification costs. POL owes the Trustee and scheme members a duty of care to provide correct data, and that duty has been breached.	It is considered very unlikely that the trustees would consider it a good use of scheme funds to sue POL. However, it is not inconceivable that they might request a contribution from POL. Consideration would need to be given to that once the entire facts are understood.	
Post Office ARA delay:	Mitigated by swift and comprehensive action to resolve errors	
Potential impact on industrial relations.	Mitigated by collaborative and open approach with Unions; and through effective communication and support provided to employed members.	
Reputational damage (at a time when the GLO is so visible via the media)	Mitigated by swift and comprehensive action to resolve errors; and by effective communication to affected members.	

7

Stakeholder Implications

- Employees: Only those who are members of the RMPP scheme may be affected. Active deferred members may have been notified of incorrect DB pension benefits. Resolution will involve specific communications (probably from both RMPP and Post Office) to these members to inform them of their correct benefits
- Pensioners: Some may have received incorrect benefits. Resolution will involve specific communications (from RMPP) to these members to inform them of their correct benefits to adjust future payment and, potentially, to request clawback of historic overpayment
- RMPP Trustee: Are responsible for managing and monitoring the Plan; they also act to ensure the members' best interests are protected. The Trustee will therefore seek a fair and equitable solution that does detrimentally affect their members. The Trustee will oversee the assessment and implementation of the appropriate solution(s).
- Post Office: As the sole sponsoring employer of the Post Office section of the RMPP it is in Post Office's interest to ensure that the existing assets of the 'closed' plan are properly managed by the Trustee to meet all future liabilities; otherwise the Trustee may seek further contribution from Post Office. There is a duty to provide correct information to the RM PSC to enable them to pay the correct benefits to members. The impact of the erroneous data provision, depending on magnitude, may require recompense from Post Office, in the form of additional contribution to the plan. Post Office will therefore wish to be closely involved in determining the appropriate solution(s).
- RM Pension Service Centre Administration Team (PSC): PSC have a duty to pay the correct benefits to members and to ensure the integrity of the data they hold. Assessment of pension impacts and correction of benefits will be actioned by PSC – thus additional resources may be required within the PSC

Confidential

POL00423570

- Unions: interest of the Unions will not only be in respect of those employed members of the RMPP scheme that may be affected, but also how the resolution will impact the release and magnitude of the existing surplus in the plan

Other Options Considered

- Resolution of the errors is not optional because of the materiality and large long tail impact on the RMPP (Post Office Section) fund - and potential call on Post Office for further contribution.

Next Steps & Timelines

- Immediate – ensure no new benefit 'crystallisation' events are based on incorrect figures (mitigating further additional pension liability)
- Continuing to early August - complete investigative work; calculate correct pensionable pay figures; detailed quantification of errors
- Late August/Early Sept - Trustee to assess impact of errors reported on individual pension benefits (output reviewed by Post Office advisers)
- Sept - For active members who are unlikely to had communication re their pensionable pay figures, we simply correct what's in the HRSC and PSC systems
- Sept – recommended future state, improved processes implemented in HRSC (and PSC)
- Sept - engagement between Post Office and Trustee leadership teams to develop and agree suitable resolution / action plan (*Note Rectification of benefits and communications with members can only be delivered by the Trustee so POL should support and encourage best practice and rapid delivery)*
- Late Sept/Oct – implementation of agree solution(s) re overstated benefits commences
- Unions will need to be engaged throughout this period.

Confidential

POL00423570

Appendix 1

- See attached Technical Appendix.

Confidential

POL00423570

Appendix – Technical Summary

Limitations

This Technical Summary is based on knowledge at 30 June 2020 – this is important. Full calculations and data checks have not been completed. Where figures are stated they should be considered initial indications only. Figures have not been reviewed by the actuarial advisers and may change materially depending on the full outcome of the investigations. Decisions should therefore not be made on the basis of this interim update.

Background

On 31 March 2014 changes were made to pensionable pay increases as part of a consultation with members (the 'Robin agreement'). From this date pensionable pay was decoupled from the pay a member actually received. The pensionable pay was increased each year by the higher of RPI (up to 5%) and permitted pensionable salary increases (limits were introduced that particularly affected people being promoted outside of their current pay grade).

A member's total pensionable salary is built up of a basic pay element and some pensionable allowances (assigned – which happen regularly e.g. a London area allowance, and intermittent – which might change on a month by month basis e.g. overtime). The Robin agreement is about pensionable pay increases only, affecting the basic pay element – whereas allowances (with one exception, detailed below) are kept separate and the actual amounts are used in the full determination of pensionable salary.

What went wrong?

Material issues found to date:

1) **Pensionable pay increases** – The data shows that in some cases a full promotional increase has been applied where the correct treatment would have been to apply none or part of the increase. Initial indications are that this issue is only present after 31 March 2017 (other than some isolated cases that have been highlighted by Pension Service Centre). It's impossible to identify who is affected by this issue without re-doing calculations for every salary increase since 31 March 2014, but we can at this point identify those with increases in excess of RPI over the period. We have identified nearly 400 members that we need to examine further, with an average salary increase of 22% **above** RPI over the period to 2020. Some of these increases will have been allowable, so we need to finish our calculations to work out which are genuine errors.

2) **Double-counting of allowances data –** Some pensionable allowances were built into the basic pay element of pensionable salary from 31 March 2014. One of these allowances (a notional pay element reflecting the POL pay deal from 2007) was correctly built into basic pay, but the others should have been kept separate in the allowances data items provided to Pension Service Centre. From 31 March 2014 - 31 December 2017, where an allowance was built into the basic pay element it was not included in the separate allowances data provided to Pension Service Centre, to avoid double-counting. This approach changed from 1 January 2018 when a new administration system was introduced in Post Office, and all of the pensionable allowances (including the notional pay element reflecting the POL pay deal from 2007) were separately provided as well as being incorporated in the basic pay element. This caused double-counting of allowances of an average of around £3,200 pa (full-time equivalent at 2018) for nearly 1,000 members.

POL00423570

Less material issues found to date:

3) **Allowances – incorporation into base pay** - some allowances (e.g. Product Specialist) have been built into the basic pay element in error. When the RPI increase calculation is done each year, the whole pensionable basic pay has been given the RPI increase, which means the allowances have also been given an RPI increase. When a member stops receiving this type of allowance, the amount of the allowance actually paid to the member is removed from their pensionable basic pay. This absolute amount deduction is likely to be different to the 'baked in' allowance in pensionable basic pay because the actual amount of the allowance being received in pay is unlikely to have received RPI increases (pay deals have typically been below RPI in recent years).

4) **Pay decreases -** some members may receive a reduction in their pay e.g. members are able to step down in grade and potentially receive other allowances that compensate them for this (sometimes for a fixed time period of say 2 years). The Rules dictate that the reduction that should be applied to the basic salary for pension purposes is the amount of the reduction in the member's actual base pay. The data shows that in some cases this full reduction was not applied to the member's pensionable salary to avoid disadvantaging the member (on the grounds that as pay increases are limited, pay decreases were limited in a similar way). However, the Rules are very clear on this point and the legal advisers have confirmed that the full reduction should apply.
   It's worth noting that in reality, another underpin to the member benefits might bite at this point rather than the new reduced pensionable pay – e.g. rules look to the best 3 year average of pay in the last 10 years of service instead of just the final year, or separate 2014/2017 underpins that are applied to benefits.

5) **Order of annual RPI increase routines** – the Rules stipulate that the RPI increase should happen first on 1 April each year, and that any pensionable pay increases after that (even if they happen on the same day) should be tested against RPI the next 1 April to determine whether any further increase to pensionable pay is required to bring up to the level of RPI. It appears from the data that this comparison may not have always happened in the right order. Recalculation of member salaries each year will be needed for the above other issues so any errors will be resolved as part of that process.

Administrative issue found to date (no impact on liabilities):

6) **Lower earnings deduction** – Section C members have the lower earnings deduction (fixed at a historic level of £3,328pa) removed from their salary as part of their pensionable pay definition. Any RPI increases should be applied to this reduced basic pay figure from 1 April 2014. Currently, figures stored on Post Office systems reflect basic pensionable pay before the reduction of £3,328 pa because calculations on the Pension Service Centre side automatically remove this lower earnings deduction as part of their calculation routines. This requirement from the Pensions Service Centre has caused data issues in the past and causes ongoing unnecessary calculation complexity on the Post Office side, because every salary calculation needs to start by removing the fixed figure, and end by adding it on again. There are known examples of these steps being missed in past calculations (which have

POL00423570

subsequently been corrected) such as RPI uplifts in 2018. The data stored by Post Office is not as per the Rules definition for basic pay from 1 April 2014; and this has caused problems with the data extract for the formal triennial valuation, as the actuarial team identified this feature and needed to adjust figures to make the appropriate deductions.
It is therefore proposed that Post Office Limited store Section C members' data in line with the Rules (i.e. with the £3,328 pa taken off from 1 April 2014) and Pension Service Centre calculation routines are amended accordingly so that they don't automatically remove the lower earnings deduction after 1 April 2014.

Data issues:

7) **Data gaps:** Post Office employee data needed for the calculations is spread across 2 admin systems – an archived SAP system (information prior to 2018) and a new Success Factors system (2018 onwards). The data from these two systems is in an inconsistent format. There are some gaps in past data (intermittent allowances like shift pay) that as yet could not be interrogated from the archived system.

   There are some 50+ pensionable allowance wage types on the Post Office systems, so the volume of related data, covering all pay increases since 2014, amounts to hundreds of thousands of lines for the members in scope for this exercise (just under 4,900 actives at 31 March 2014). Rebuilding any missing data is challenging and, in some cases if data cannot be obtained from the system, near impossible. Some pragmatism will need to be adopted, we are unlikely to be able to simply restate all pensionable salary and allowance data since 2014.

Why did things go wrong?

Complexity – The changes made to pensionable pay increases in 2014 were complex. This is partly because they were the end result of a consultation so reflected a position that was different to the simpler initial Company proposal. Documentation was insufficient to support the operation of the new changes. This has introduced risk of human error where manual calculation is required and inappropriate system configuration.

What does this mean?

Effect on buy-in data

There is nothing in our findings so far to indicate that there is a material issue with the buy-in data, because the material problems originated after the data extract for the buy-in was taken.

Effect on actuarial valuation

Although the triennial actuarial valuation was carried out in 2018, the allowances data was taken from the old admin system, so the double-counting issue should not affect the results of the actuarial valuation (and is also why the error wasn't identified at the time). There will be a limited impact from the pensionable pay increases issue for increases received between 31 March 2017 and 31 March 2018, and from the less material issues covered above.

POL00423570

Effect on member benefits

The effect on member benefits depends on whether a member is still employed (active), has left employment (deferred), retired or died. The table below shows a breakdown of the two material issues and the split of member status as at 30 April 2020. The table does not show a breakdown of the less material issues, so further members may be impacted, but these will be identified as part of the complete recalculation of pensionable salary history.

Current status of member at 30 April 2020	**No. of members with *potential* pensionable salary increase issues**	**No. of members with double counted allowances at 1 Jan 2018**	**Notes**
Active	281	369	Members may never have been communicated their incorrect salaries – therefore correction much simpler.
Deferred	56	325	Members likely to have been communicated incorrect benefits at the point they left
Part/fully-retired	45	288	Members likely to be receiving incorrect benefits
Died	3	4	Members likely to have received incorrect benefits
Total	**385**	**986**	

7

What have we done so far?

Benefit summary - documented how the salary calculations should be carried out

We have discussed, agreed and documented how the salary calculations done by Post Office should be carried out. This summary is in the final stage of being agreed by the Trustee and Company legal advisers.

Individual member checks

A number of individual member calculations have been carried out, comparing data held on Post Office systems to data held on Pension Service Centre systems. This helped us identify issues with the calculations.

Process review

Post Office have conducted a detailed review of processes to make sure that things are done efficiently and correctly going forwards. New processes will be implemented at the same time as any corrections are made to active member data. Going forwards, pensionable salary calculations will be done using an automated spreadsheet rather than manually.

Administrative practice identified

Discussions with Post Office personnel and examination of past spreadsheets and documents have identified how calculations are done in practice, where the Rules or Post Office Policy do not dictate how the calculation should be carried out. This has been incorporated in the document agreed with the legal advisers.

POL00423570

Pensionable salary calculator

A pensionable salary calculator has been built in Excel to do calculations going forwards. This will be reviewed by the Company's actuarial adviser.

Data gathering and checks

Pensionable salary and allowances data has been obtained from the old and new admin systems on the Post Office side, and from Pension Service Centre. Initial data as at 31 March 2014 from Post Office systems has been checked for reasonableness and queries resolved. Data reasonableness checks for salary increase data from 2014 to 2020 is underway.

Rebuilding pensionable salary calculations

Work is underway to rebuild the pensionable salary calculations for around 4,900 members, for all changes to salary since 31 March 2014. This work will be reviewed by Post Office's actuarial advisers once it is complete.

What are the next steps?

1) Final signoff of benefit summary
2) Post Office to finish rebuilding pensionable salary calculations and obtain actuarial review
3) Compare results of rebuilt salary calculations with salary data held by Pension Service Centre as at 31 March 2017 (date of buy-in extract) and recent 2020 data extract.
4) Trustee's actuarial adviser to quantify the liability impact at 31 March 2017 and 2020 (and potentially any liability impact on the actuarial valuation if anticipated that it may be material)
5) Trustees to decide on approach to correcting data and how to communicate this to members
6) Data corrections (including any further calculations as a result of Trustee approach) to be carried out, and new processes introduced to minimise risk going forwards.

POL00423570

POST OFFICE LIMITED RCC REPORT

Title:	The Current Operation of Suspense Accounts	**Meeting Date:**	13 July 2020
Author:	Mark Underwood, Tom Lee & Tim Perkins	**Sponsor:**	Ben Foat & Alisdair Cameron

Input Sought:

The RCC is asked to **note**:

- The findings from KPMG's review of Post Office's current operation suspense accounts.

The RCC is asked to **approve** the recommended approach:

- Whereby KPMG are instructed to explore whether it is possible to perform the same independent review, but for Post Office's historical operation of suspense accounts.

Previous Governance Oversight

- Post GLO Settlement Programme SteerCo of 1 July 2020

8

Executive Summary

1. Allegations continue to be made that Post Office may have recovered sums from Postmasters (including through civil and criminal proceedings) which were not 'real losses' to Post Office as they were housed in suspense accounts and taken to profit by Post Office.
2. KPMG were instructed to review Post Office's current operation of suspense accounts. Although their findings include a number of points to consider in terms of how Post Office could enhance best practice. In summary, given the robust and transparent investigations process that is undertaken, these suspense accounts should not result in Post Office pursuing Postmasters for sums it had or could eventually take to profit. This is because sums housed in suspense accounts are either:
   - not taken to a profit and loss account; or
   - relate to unmatched transactions due to customers (not postmasters); or
   - relate to surpluses rather than shortfalls.
3. BAU investigations and the Historical Shortfall Scheme provide mechanisms whereby shortfalls can be investigated and/or resolved. However, this is unlikely to satisfy Post Office's detractors.
4. Thus, and at a cost of c£47k, it is recommended that the RCC approve instructing KPMG to explore whether it is possible to perform the same type of independent review, but for Post Office's historical operation of suspense accounts.
5. The RCC should note that any documentation which is produced and findings made, may be disclosable as part of Post Office's ongoing disclosure obligations to those it has prosecuted historically and as part of any future claims made against Post Office as a result of historical practices, in both a civil and criminal context and in the context of any relevant investigation or inquiry.

Confidential

POL00423570

Questions addressed

1. What is a suspense account? What allegations have been made in respect of how Post office operates suspense accounts?
2. What assurance does KPMG's review give Post Office? What were the findings?
3. What options exist to Post Office for managing any historical and future suspense account related claims?
4. What further work could KPMG perform over the historical operation of suspense accounts? How much would this cost? What are the limitations and risks?

Report

History & Context

1. Post office uses suspense accounts:
   - To house branch discrepancies arising as part of the normal course of trading and which need to be cleared at the period end (either surplus or deficit).
   - To house surpluses arising from Postmasters where the Postmaster does not agree the surplus is due back to them.
   - To temporarily hold differences in payments moving between Post Office and its clients, where the client and Post Office's view of what is payable or receivable differ. Differences are investigated but in some cases neither Post Office, the client, nor the branch are able to determine the identity of the customer who performed the transaction in question or the specifics of the transaction. For example, Post Office may not be able to determine the details of the bank account to be credited. In such situations, and following enquiries with branches, unresolved differences are moved to Post Office customer creditor suspense account. Such discrepancies are held in its suspense account to give time for customers and other parties to put forward more information to explain what has happened.

2. A long standing assertion, made by applicants to the Complaint Review & Mediation Scheme, Claimants in the GLO, and by Lord Arbuthnot is that:
   - Post Office operates one or more suspense accounts in which it holds unattributed surpluses including those generated from branch accounts;
   - After a period of time, such unattributed surpluses are credited to Post Office's profits; and
   - Post Office therefore has recovered (through civil or even criminal proceedings) sums from Postmasters which were not real losses to Post Office, as they were housed in suspense accounts and ultimately taken to profit by Post Office.

3. These allegations were first made in the context of the Complaint Review & Mediation Scheme[1]. Second Sight's[2] final report, published in 2015, claimed they had been informed that at each year end, substantial unreconciled balances existed on many individual suspense accounts and that these unreconciled balances for the 2014 financial year were approximately £96 million in respect of Bank of Ireland ATMs and approximately £66 million in respect of Santander. They said that "*these unmatched balances represent transactions from individual branches that occurred in the preceding 6 months*" and they "*...remain*

1 'Project 'Sparrow' which, broadly speaking ran from 26 August 2013 – 01 February 2016.
2 The firm of independent forensic accountants instructed to investigate each of the applicants cases accepted into the Scheme

POL00423570

concerned that these balances may include transactions that ultimately should be credited back to individual branch accounts".

4. In its 'Reply' to the Second Sight Report, Post Office stated that Second Sight had misunderstood the information provided by Post Office. The balances of £96m and £66m were taken from routine trading balances yet to be settled with other organisations at a particular month end. In other words, they represented amounts due to other parties, not amounts that were unreconciled and which may be due to Postmasters.

5. Second Sight were also provided with details of the credits released from Post Office's suspense accounts to profit for the period 2008 to 2013. As there was a 3 year retention period – no amounts at that time had been released for the years 12/13 and 13/14. The total gross credits released from suspense to profit from 2007/8 onwards was as follows:

Years released to profit	Value
2010/11	£612,000
2011/12	£207,000
2012/13	£234,000
2013/14	£104,000
2014/15 (YTD at the point provided)	£8,000

6. In its reply to Second Sight, Post Office stated that amounts should be considered within the overall context of Post Office performing around 2.5 billion transactions per annum, with a combined value in the order of £60bn. The amount of unresolved credits that end up in Post Office's P&L (at the time) was therefore less than 0.001% of all transactions (by value) undertaken by branches.

7. Allegations continue to be made in respect of Post Office's suspense accounts. In February 2020 Lord Arbuthnot wrote to Nick Read. In Nick's response, he committed to better understanding how Post Office operates its suspense accounts. Nevertheless, in the House of Lords on 18 June 2020, Lord Arbuthnot complained that the Terms of Reference for the recently announced 'Independent Review into the Post Office Horizon IT System and Trials' do not "*say anything about the likelihood of the Post Office improperly making a profit from the sub-postmasters, or about the suspense accounts*".

KPMG's Suspense Account Review

8. KPMG were instructed to review how Post Office currently operates its suspense accounts. The scope of this review was as follows:
   - Confirm the number of relevant suspense accounts operated by Post Office into which sums are placed which could, theoretically, relate to discrepancies at a branch level and from which any unmatched sums may be taken into a Profit and Loss (P&L) account.
   - For these accounts, assess whether how they are operated reflects the associated documentation and best practice.
   - Identify whether there are any gaps / challenges within existing processes which could result in risk to Post Office and or Postmasters.

Confidential

POL00423570

- Assess whether the current resolution criteria adopted by Post Office for dealing with discrepancies appears 'fair and reasonable' to both Post Office and Postmasters, based upon KPMG's understanding of best practice.
- Comment on any further work that Post Office might want to consider.

KPMG's Findings

9. KPMG identified 4 relevant suspense accounts which are currently operated by Post Office; details of which are provided within the table on the following page. In summary, given the robust and transparent investigations process that is undertaken, these suspense accounts should not result in Post Office pursuing Postmasters for sums it had or could eventually take to profit.

10. This is because sums housed in suspense accounts:
    - are either not taken to a profit and loss account; or
    - relate to unmatched transactions due to customers (not Postmasters); or
    - relate to surpluses rather than shortfalls.

11. For completeness and although purely hypothetical, included at **Annex 1** is a worked example for how a postmaster could repay a shortfall which Post Office has or eventually could take to profit via a suspense account. Post Office is not aware of any examples of this having taken place and it requires, for example:
    - a Postmaster not following process;
    - refunding a customer, prior to an investigation taking place and without contacting Post Office;
    - not recording the refund on Horizon; and
    - not recalling the refund during the subsequent investigation.

    Owing to its nature therefore, it would extremely difficult if not impossible for Post Office to prevent.

POL00423570

Account	Description	Houses Deficits and or Surpluses?	Postmaster Affecting?	Are unmatched sums taken to P&L?	KPMG Findings Summary
Branch Snapshot. Current Balance: £355,204	This is a holding account within branch accounts which allows Postmasters to investigate discrepancies that have arisen within their branch without the need to recognise and potentially settle the amount at their trading period end.	Deficits and Surpluses potentially due to Postmasters	Yes	**No**. These accounts relate to discrepancies identified by Postmasters and which result in a Postmaster either repaying (deficit) or being repaid (surplus) amounts. Resolution of these discrepancies is either in cash or via Postmaster's personal accounts in the Group Ledger.	**Branch Deficits** KPMG's assessment is that Post Office are moving towards best practice. There is an established, robust and timely investigation and resolution process which is undertaken in conjunction with Postmasters and the development of a tailored training course encompasses the key aspects of best practice. In addition, the level of monitoring and oversight is robust ensuring there are no unauthorised transactions and aged balances do not build up. Whilst operational documentation provides Post Office with a clear audit trail, there is a lack of formal detailed process documents and inconsistencies between documented and actual practices. **Branch Surpluses** Policy and procedures are unclear and Postmasters are not routinely informed when surpluses arise on their personal accounts in the Group Ledger. The timeliness of repayment is dependent upon the value of the surplus and is in direct contrast to the branch deficit policy. There is a currently a backlog into investigations of surpluses and monitoring of branch surpluses is inconsistent.
Local Suspense. Current Balance: £0	Branch discrepancies arising at the period end are posted to this account. The balance on this account must be cleared before the branch can complete their period end roll over. Depending on the value of the discrepancy, the balance is either made good through the Postmaster putting cash into the office (if less than £150) or can be 'settled centrally' (if over £150) meaning the balance is moved in to the Postmaster's personal account in the Group Ledger. Discrepancies can be investigated after they are made good or posted to the Postmaster's personal account in the GL				
Agent Creditor. Current Balance: £17k	This account holds **surplus** discrepancies which Post Office believes are due to Postmasters, but that Postmasters dispute being due to them.	Surpluses potentially due to Postmasters	Yes	**Yes**. This accounts house surpluses from which unmatched items can be released to the Post Office P&L account after 5 years. However, as this account relates to surpluses which are disputed by the Postmaster (as opposed to	Formal policies in place regarding when amounts can be released to the P&L account. Though operational policies are clearly understood, they are informal and not yet fully documented.

Confidential

POL00423570

Account	Description	Houses Deficits and or Surpluses?	Postmaster Affecting?	Are unmatched sums taken to P&L?	KPMG Findings Summary
				Post Office) any improper operation should not result in Post Office potentially pursuing Postmasters for monies it had already or could eventually take to profit	
Customer Creditor: Current Balance: £3.5m	This account holds amounts repaid to Post Office from third parties due to issues identifying who the money is owed to. Third parties include Santander, MoneyGram and Camelot customers. Amounts are held in this account, pending inquiry from the customer.	Surpluses potentially due to customers	No. These monies relate to customers who cannot be traced due to inaccurate data.	**Yes**. This account houses surpluses from which unmatched items can be released to the Post Office P&L account after 6 years or earlier where specific policy is to do so. However, as this account relates to unmatched sums potentially due to customers (as opposed to Postmasters) any improper operation should not result in Post Office potentially pursuing Postmasters for monies it had already or could eventually take to profit.	An established level of best practice in respect of documentation, monitoring and resolution. A good level of operational documentation provides a clear audit trail and monitoring ensures there are no unauthorised transactions to or from the account. All amounts posted in this account are investigated with the relevant branch prior to being posted in this account. No evidence that amounts posted to this account would relate to branch discrepancies which were previously repaid by a Postmaster.

POL00423570

Recommendations Included within the KPMG Review

12. The KPMG report includes a number of points to consider in terms of how Post Office could improve its operation of suspense accounts to enhance best practice. These include:

- Implementing and documenting policies and procedures including details of ownership, format, content and version control for all relevant suspense accounts.
- Ensuring all processes are adequately documented and that policies are consistently applied within the documentation.
- Implementing an overarching branch discrepancy process document linking all relevant policies and processes.
- Formalising the reporting and review by senior management of suspense accounts and investigation outcome metrics.
- Undertaking a review of the branch deficits written off centrally to identify whether any Postmasters are regularly benefitting from the policy.
- Reviewing the policy and process for branch surpluses with specific focus on:
  i. Communicating surpluses to postmasters.
  ii. Repayment timescales not being determined by value.
  iii. Timeliness of investigation process.
  iv. Aligning the branch deficit and branch surplus policies and expectations.
- Implementing a process to address the current backlog that has arisen in the investigation of branch surpluses and the resolution of old branch surpluses that are in dispute to ensure:
  i. Repayments are made in a timely manner; and
  ii. Where appropriate, amounts are moved into the Agent Creditor Account.

13. All recommendations are being taken forward, and will be implemented through BAU over the course of the 20/21 financial year.

Next Steps

14. Although the KPMG report gives Post Office assurance that its current operation of suspense accounts should not result in sums being pursued from Postmasters which Post Office has already or could also take to profit via a suspense account, the scope of the review did not include Post Office's historical practices.

15. If a historical error, in relation to the operation of suspense accounts, was to adversely affect a branch, this would almost certainly manifest itself as a shortfall. The Historical Shortfall Scheme provides a mechanism for shortfall claims to be investigated. The only caveat to this is if their claim relates to a period of time for which the branch in question was operating on HNGA. This is because HNGA related claims are ineligible for the Scheme.

16. However, any such 'suspense account related claim' which relates to a period during which HNGA was in operation at the branch in question would still manifest itself as a shortfall and can therefore be investigated through current BAU processes (which KPMG have found to be transparent and robust).

POL00423570

17. Nevertheless, this is unlikely to satisfy Post Office's detractors and the allegations will continue. As such it is recommended that the RCC approve instructing KPMG to explore whether it is possible to perform the same independent review, but for Post Office's historical operation of suspense accounts. It may not be possible, owing to the timeframes involved (2000 – 2019), key personnel no longer being in the business and documentation being destroyed in line with retention schedules (prior to legal holds being in place). KPMG has provided a cost estimate of £47k to complete this work.

18. If it is possible, the RCC should note that any documentation which is produced and findings made, may be disclosable as part of Post Office's ongoing disclosure obligations to those it has prosecuted historically and as part of any future claims made against Post Office as a result of historical practices, in both a civil and criminal context and in the context of any future investigation or inquiry.

Confidential

POL00423570

Annex 1 – Theoretical example for how a Postmaster could repay a shortfall which Post Office has or eventually could take to profit via a suspense account[3]:

Step	Customer balance	Branch balance	Postmaster balance	POL balance	Bank balance
A customer makes a £10 deposit in branch.	£0	£0	£0	£0	+£10
The customer complains the deposit has not been received in the associated banking account. By way of an example, this could be as a result of the Postmaster incorrectly recording the account details on Horizon.	-£10	£0	£0	£0	+£10
The Postmaster chooses to refund the customer £10, without recording it on Horizon	£0	-£10	£0	£0	+£10
The bank refunds £10 to Post Office.	£0	-£10	£0	+£10	£0
Prior to Post Office moving £10 to its Customer Creditor Account, Post Office investigates with the branch in question any sums originating from transactions performed within that branch. If the Postmaster does not recall refunding the customer - the £10 would be moved to the Customer Creditor Account.	£0	-£10	£0	+£10	£0
At the end of the trading Period (having still not recalled refunding the customer) the Postmaster chooses to make good the £10 shortfall.	£0	£0	-£10	+£10	£0
If after 6 years the amount remains unmatched, it is released to Post Office's Profit & Loss Account	£0	£0	-£10	+£10	£0
Thus, Post Office has received £10 from the Postmaster but still houses the original £10 within its Customer Creditor Account	£0	£0	-£10	+£10	£0

8

[3] For simplicity, this table ignores any applicable transaction fees.

Confidential

POL00423570

POST OFFICE LIMITED
COMMITTEE REPORT

Title:	Law & Trends Report	**Meeting Date:**	13 July 2020
Author:	Sarah Gray (Legal Director)	**Sponsor:**	Ben Foat (General Counsel)

Input Sought:

Noting:

The Board is asked to note the new or proposed material changes to laws and regulations this month.

Previous Governance Oversight

None.

Executive Summary

There are 3 matters for the Committee to note (details of which are set out in the Appendix):

1. Employment Legislation Update (COVID-19)
2. ATM Additional Business Rates Update
3. Public Sector Bodies (Websites and Mobile Applications) (No.2) Accessibility Regulations

Those matters that relate to Covid-19 are continuously monitored to assess the short and long term risks and potential impact to the Post Office through the relevant working groups that have been stood up and a robust governance framework.

With regard to the other matters referred to, significant work has already been undertaken to ensure any material risks that may arise for the Post Office are being managed to ensure compliance. Where no action is required, the matter has been noted and any further developments will be reported on.

Strictly Confidential

POL00423570

Appendix 1

1. Law & Trends Report: New material updates

Issue	Why it matters?	Latest Developments	Impact on Post Office	Action	RAG
Employment Legislation Update (COVID-19)	Due to the impact of COVID-19, there have been many legislative changes in the employment landscape in order to accommodate and effectively react to the changing requirements. The Coronavirus Act 2020 was introduced by the Government on the 19 March and came into force on the 25 March. The Act introduces emergency powers to handle the COVID-19 pandemic, and out of this introduces several employment changes. There has also been changes made to existing employment legislation.	In the May RCC Law & Trends report, updates were provided on the following legislation: a) Coronavirus Job Retention Scheme ('JR Scheme') b) Emergency Volunteering Scheme ('EV Scheme') – c) Working Time (Coronavirus) (Amendment) Regulations 2020 – Carry-over of Annual Leave This regulation was brought in very quickly and the expected subsequent guidance and legislation failed to appear. With the easing of lockdown it appears unlikely that this will ever materialise and focus is on how Post Office can support the easing of lockdown for those that wish to return to work.	Although work was undertaken to explore whether Post Office would want to take advantage of the JR Scheme, the decision was made not to furlough anyone and in any case the JR scheme has closed to applicants now. The focus for Post Office is on supporting people returning to work through the exceptional circumstance policy and ensuring the workplace is compliant with all the COVID-19 related guidance. As it stands, HR have received 10 requests from employees regarding returning to work. Risk assessments are taking place and the Health & Safety Team are heavily involved in working through the results of these.	The relevant working groups continue to work through government guidance as and when it is being published to ensure Post Office is compliant. Post Office policies and guidance are being updated regularly and disseminated throughout the business as appropriate.	
ATM Additional Business Rates Update Appeal of Cardtronics UK Limited and others v Sykes and others	The appeal concerned the treatment of ATMs for business rating purposes situated in supermarkets or shops owned and operated by the retailers. The Valuation Office Agency ('VOA') changed its practice in 2010 and started to assess ATMs separately for additional business rates where they did not form a part of a bank branch. There were two main issues:	In 2014, due to the unique contractual arrangement of Post Office and Bank of Ireland, Post Office received a confirmation letter from the VOA that they would exercise its operational right to not separately assess Post Office ATMs and therefore Post Office didn't have to pay additional rates on separately assessed ATMs. However, in 2018 the VOA changed their appeals system meaning that Post Office could no longer rely on this letter and therefore since 2018 has been incurring	Now that the Supreme Court has made final judgment and no further appeals can be made, the effect of that decision means that Post Office can move forward in escalating and challenging the ATMS that were assessed separately and claiming a rebate. There are approximately 53 ATMs that Post Office have been paying ATM rates on that total £354k; we are unable to claim for the backdated charges from 2014-2017 meaning Post Office are only entitled to claim back £297k. The backdated charges	Post Office has already engaged with Bank of Ireland, however is also going to engage with the VOA to ascertain whether there is a one-off exercise that can be undertaken centrally due to the unique contractual relationship with Post Office and Bank of Ireland in relation to ATMs to address the rebate. Rates are usually paid pending a challenge and the Rates Bill for 2020/2021 for England & Wales ATMs would total £109,000. Post Office is also going to enquire as to whether these rates can be put on hold to avoid	

POL00423570

Issue	Why it matters?	Latest Developments	Impact on Post Office	Action	RAG
	1) Whether the sites of the ATMs are to be properly identified as separate hereditaments from the stores 2) Who was in rateable occupation of the separate hereditaments and therefore responsible for the additional business rates	charges on around 53 ATMs totalling £354k. Due to the ongoing case, Post Office was advised to wait for the outcome before escalating this situation.	were in a different valuation roll and therefore had to be challenged by 31 March 2018, following advice to wait for the outcome of the case to challenge, we are now unable to claim back for this amount. Rebates are completed via the on-line system, but only the occupier for the site of the ATM can register for an account in order to make these challenges; legally Bank of Ireland are the occupier and therefore will need to register themselves, although it is Post Office who will be entitled to the refund as it is Post Office who have incurred the cost.	paying this payment and then having to claim a rebate in quick succession.	
Public Sector Bodies (Websites and Mobile Applications) (No.2) Accessibility Regulations (the 'Regulations')	The Regulations introduce obligations for Public Bodies to make websites and mobile applications accessible for people with disabilities. Complying with accessibility standards has always been best practice for designers and developers however due to various factors it became hard to oversee and compliance with the standards dropped. The Government has now introduced the standards as law which has effectively forced the hand of public sector bodies to comply.	Accompanying government guidance to the regulations states websites and mobile applications will comply if they meet the WCAG2.1AA Accessibility Standards. The standards identify issues and set standards for ensuring websites and applications can be used by disabled people, taking into account both their disability and the equipment or software they may use as an aid. Some examples are: - Ensuring a website can be navigated using a keyboard rather than a mouse; - Avoiding use of certain problematic add-ins; - Making sure image size and quality is appropriate; and - Ensuring adequate colour contrast to make test and images legible to the visually impaired. A public body does not have to comply where compliance would impose a 'disproportionate burden'. To determine a disproportionate burden, the public body must consider its own size and resources, the cost and difficulty of the remediating measures and the benefits which implementing these remediating measures would provide for a disabled user.	The Regulations apply to Post Office as a 'body governed by public law'. **Obligations for accessibility will apply to Post Office's websites from 23 September 2020 and to its mobile applications from 23 June 2021.** Although some organisations are contractually obliged to meet these standards or self-accredit, formal compliance with the standards is new for Post Office. Post Office has done the following in order to address the introduction of the Regulations: - A period of insourcing talent to ensure consistency across digital design and development and greater oversight; - Changing the procurement process so the on-boarding includes references to compliance to web standards and accessibility; and - Bringing in AbilityNet to carry out a third party audit to assess the extent of the accessibility issues. The results of the audit showed that across the core touch points of the Post Office websites and high level across the whole	The Digital Innovation Team's view is that come September, Post Office will be in a good position with respect to compliance with the Regulations. Further work will continue to engage with sub-contractors and stakeholders as appropriate. The Digital Innovation team is also looking to engage several charities such as Mind, to complete testing on the new designs. Mobile applications have to be compliant by 23 June 2021, and although the priority is the website, budget has been allocated for an audit by AbilityNet on the Post Office mobile applications.	

POL00423570

Issue	Why it matters?	Latest Developments	Impact on Post Office	Action	RAG
		The public body must also produce an Accessibility Statement. This must include details of which parts of the website are not accessible and why, as well as contact details so a user can both notify the body of any failures to comply with the Regulations and request a copy of any information a disabled user cannot obtain as a result of such failures.	site there were 1000 accessibility issues. In order to address all issues the core platform of the Post Office website would have to be created from scratch and therefore Post Office's approach is to address all the accessibility issues that it possibly can. The Digital Innovation team is working closely with Legal and Compliance in order to get to a position where there is comfort that Post Office has remediated everything it can and be confident in the Accessibility Statement that it produces. It has also been identified that Post Office doesn't own the code for all its digital platforms Corporate Website etc.) which leaves Post Office with no ability to address accessibility issues. The Digital Innovation team is engaged with Legal and Compliance in order to address how we can engage those stakeholders in relation to the Regulations.		

POL00423570

POST OFFICE LIMITED
RISK COMMITTEE REPORT

Title:	Procurement Governance & Compliance Report	**Meeting Date:**	13th July 2020
Author:	Barbara Brannon, Procurement Director	**Sponsor:**	Alisdair Cameron, Group Chief Financial Officer

Input Sought: Noting

Noting – For discussion and further action if required.

Previous Governance Oversight

- May 2020 - Quarterly Risk Report

Executive Summary

As a business in receipt of public funds POL is bound by the Public Contract Regulations (2015). PCR 2015 oblige POL to behave in a fair, objective & transparent way when contracting with 3rd party suppliers. Additionally, set procedures must be followed for spend above £25k and £189k.

The purpose of this report is to set out both breaches to Post Office governance and key controls around contracts and compliance to PCR regulation in the award of contracts.

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

From March 2020, Post Office Board has requested prior approval of all Exceptions >£189k in a revision to existing governance. A Procurement Risk Exception Note will be required to accompany all Exception Requests and a Legal Risk note for requests >£500k, and/or with Exemptions or with Medium/High Risk of challenge.

POL00423570

Questions addressed

1. *How many and what types of procurement risk exceptions have occurred in the past quarter?*

   Since the last RCC report at the beginning of May there have been 8 Procurement Risk Exceptions which have been submitted to Board for approval:

   a) 2 are interim extensions for ATM support
   b) 1 relates to software support which cannot be procured compliantly
   c) 2 relate to Banking services
   d) 1 relates to GLO audit services
   e) 2 relate to professional services

   Furthermore, the 6 month contract extension period for Global Payments has now commenced increasing the value of the open risk. This risk exception was approved in March.

   A list of these awards is set out at the beginning of Appendix A.

2. *What are we doing about it?*

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

   Our overall non-compliance value has increased from £19.5m in May [£21.01 in March] to £27.7m in May.

   A visual breakdown on Open incidents is available in Appendix A.

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

   a) £10m. **EUC** - A project has been initiated to re-procure End User Computer services for both Branch and Colleague Services. The current plan is to have a new supplier(s) in place before the end of the current contract [April 2021 with 2 years exit services] with a targeted migration by April 2023. The project is currently gathering requirements to go to market however, the exit assistance period is the subject of a Legal Risk Note.

   b) £1.6M **VARIOUS** - IT have three hardware and software support contracts valued at circa £1.6m expiring in August. This is proprietary hardware and software which cannot be supported by other manufacturers. There is currently no exit roadmap for the equipment and services which are not end of life. A compliant route has been identified for the two hardware contracts but this will attract a management fee of up to 10%. A Procurement Risk Exception Form has been prepared for GE to discuss.

POL00423570

Conclusion

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

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

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

Report

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

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

   Procurement Risk Exceptions may be made for a number of reasons at the Post Office.

   a) Low value, time constrained or highly sensitive/specialist engagements occur from time to time. Firms are sometimes "conflicted out" from some work due to previous engagements.
   b) Large commercial arrangements cannot often be easily competed or unravelled without operational impact, and re-procurement may be subject to a pending evolution of a supporting Business Strategy and/or completion of large, and complex technical programmes of work to maintain or enhance services prior to a possible exit.
   c) The contractual arrangements may pre-date PCR 2015 regulations or the contract novated during separation from RMG, automatically becoming non-compliant at the renewal point. Non-compliant awards are frequently made on a tactical basis to extend contractual services while public tender processes are executed.
   d) Delays to public sector supplier panels becoming available. The Post Office makes extensive use of this low-cost route to market and new/refreshed panels are subject to frequent delays from Crown Commercial Services. Single interim extensions [of periods under 12 months] while tender processes are run are considered to be low risk legally.

POL00423570

e) Changes in scope or value over the term of a contract may render the extension or renewal of services non-compliant. Material changes to the scope of a contract may render the whole contract non-compliant.
f) Disregard for, or lack of understanding of the regulations.

3. Why are we receiving this report?

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

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

A full explanation of the individual compliance breaches for direct awards over £189k [previously £164k & £181k] threshold is attached in Appendix A. Each entry details the nature of, and the value of the breach. The threshold is altered annually based on the FX rate between GBP and the Euro.

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

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

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

All contracts entered into during this period were compliant with internal governance processes on contract and commercial review.

6. *Why were the approvals given?*

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

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

There were no unapproved, material breaches during this period.

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

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

POL00423570

b) Sourcing options papers are prepared for review by contract managers and key stakeholders [risk, legal, security] with routes to market agreed. In many cases these are dependent on evolving business and operating model strategies and the Procurement team are actively involved helping to advise and review options as thinking evolves.
c) Where a non-compliant award is proposed due to time pressure, Procurement are actively working on long term mitigation with awards made on an interim basis to meet urgent operational needs.
d) Each RCC member now receives a regular report on compliance within their business unit[s].
e) A Risk & Governance process requires a Risk Exception report to be created for non-compliant direct awards with GE sign off.
f) Awards over £189k must have prior Board approval before being entered into.
g) All Professional Services engagements must be approved in writing in advance by the CFO/COO. A compliant panel of preferred consulting partners has been appointed and proposed engagements outside of this panel are subject to additional review and challenge.
h) Procurement provides training as part of the revised Induction process for new staff. Training packs are being updated for existing staff and a new training module made available on Successfactors. Ad hoc training sessions for interested Business Units are also run.
i) A new Intranet site has been launched for Procurement to improve visibility of process, regulation, and the panels of approved compliant suppliers available to POL business units.
j) A revised POL Procurement Policy and supporting processes is in progress giving more granular guidance.
k) Using Crown Commercial Services frameworks, panels of Preferred Suppliers are being refreshed and updated across a wide range of spend categories to reduce time to market, improve compliance and greatly improve commercial outcomes and legal risk.
l) A planned change to operational systems will, once live, give Procurement earlier visibility of potential compliance issues eg: contractual value thresholds.

10

Risk Assessment, Mitigations & Legal Implications

1. As a business in receipt of public funds POL is bound by the Public Contract Regulations (2015). PCR 2015 oblige POL to behave in a fair, objective & transparent way when contracting with 3rd party suppliers. Additionally, set procedures must be followed for spend above £25k and £189k.
2. Failure to abide by the legislation or "slicing and dicing" contracts exposes POL to risk, both as far the commercial outcomes of the contracts as well as the reputational damage, legal remedies, censure & fines that can follow the discovery of a breach. Our compliance to PCR can be requested under a Freedom of Information request at any time.
3. The PCR Compliance Register allows for the tracking of breaches to PCR regulations at the Post Office and internal governance processes. One aim of collating this information is to drive improvement in awareness and compliance behaviour across the organisation. The second and primary aim is to work with GE and Business Units to commence commercial reviews in a more timely way ensuring POL obtains value, commercial and contractual flexibility fitting the requirements and business strategy of the organisation.

Strictly Confidential

POL00423570

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

POL00423570

Appendix A – All Open Material Incidents

Date	Procurement Category	Function	GE Member	Supplier Name	Value/ Income	Risk Rating	Mitigation	Breach Type 1 - PCR Threshold	Reason for Breach
23/03/2017	Professional Services	HR	Lisa Cherry	Various	£ 800,000		In flight	PCR OJEU level	Requirements and HR personnel changed. OLD PSL fell into disuse.
10/01/2018	IT Software	Retail & Franchise	Amanda Jones (interim)	NCR	£ 1,800,000	Low	Pending	PCR OJEU level	Annual maintenance and support provided under Regulation 32 exemption for IPR. Tender planned for new systems/software in 2020/21 subject to funding.
23/04/2018	Marketing	Marketing & Brand	Emma Springham	CACI	£ 600,000	Medium	Pending	Medium threshold	Was a previous compliant contract - now extended non compliantly .
19/10/2018	Identity Services	Identity Services	Owen Woodley	Digidentity Services	£ 920,000		Pending	PCR OJEU level	Variation to non compliant contract to reduce charges following UK Verify changes
18/12/2018	IT Software	Financial Services	Owen Woodley	Space Between	£ 250,500	Low	In flight	Medium threshold	CRO Optimisation Services on POL website which have organically grown in value over time. Compliant process has now been run with service transitioning to new provider in April 2020 subject to contract. Interim extension entered into in February to provide services until a cutover can be completed.
04/01/2019	Digital Services	Financial Services	Owen Woodley	Webhelp	£ 321,000	Low	In flight	PCR OJEU level	Current contract expired 14/12/18. Retrospective extension was prepared but not executed (to 31/12/19). Services have now ceased with full and final settlement letter to be drafted with legal for Services to 06/01/20. There have been no final costs/claims yet submitted by WebHelp (29/04/20) so POL has not been able to confirm "full and final settlement" letter.
05/03/2019	Marketing	Marketing & Brand	Amanda Jones (interim)	Two Visual	£ 50,000	Low	Pending	Medium threshold	Business Preference. Contract and internal governance retrospectively completed.
27/03/2019	Goods for Resale	Retail & Franchise	Owen Woodley	Vow Retail Ltd	£ -	Low	In flight	Lower threshold (PCR not applicable)	INCOME £450: Contracts for wholesale and online channels were renewed under existing existing contracts which were advertised under PCR and without stand alone contracts being put in place (this action would bring them into compliance as neither fall inder CCR or PCR).
15/06/2019	Marketing	Marketing & Brand	Emma Springham	RAPP/ CODE	£ 1,000,000	High	In flight	PCR OJEU level	OJEU expired
14/11/2019	Management consultancy	Finance	Nick Read	McKinsey	£ 2,000,000	Low	None	PCR OJEU level	Business Preference. Contract and internal governance retrospectively completed.
28/11/2019	Management consultancy	Finance	Nick Read	McKinsey	£ 250,000	Low	None	PCR OJEU level	Business Preference. Contract and internal governance retrospectively completed.
23/12/2019	PR	Corporate Affairs & Comms	Nick Read	Cardew Group	£ 127,000	Medium	None	Medium threshold	GLO Response. Business Preference. Contract and internal governance retrospectively completed.
30/12/2019	Digital Services	Retail & Franchise	Amanda Jones (interim)	Abcomm	£ 42,000	Medium	None	Medium threshold	Business Preference. Contract and internal governance retrospectively completed.

Strictly Confidential

POL00423570

Date	Procurement Category	Function	GE Member	Supplier Name	Value/ Income	Risk Rating	Mitigation	Breach Type 1 - PCR Threshold	Reason for Breach
30/12/2019	Digital Services	Retail & Franchise	Amanda Jones (interim)	9XB	£ 30,000	Medium	None	Medium threshold	Business Preference. Contract and internal governance retrospectively completed.
30/12/2019	Comms, R&I & PR	Corporate Affairs & Comms	Richard Taylor	Kantar	£ 52,000	Low	Pending	Medium threshold	Business Preference. Contract and internal governance retrospectively completed.
30/12/2019	Market Research	Corporate Affairs & Comms	Richard Taylor	AB Publishing	£ 100,000	Low	Pending	Medium threshold	Business Preference. Contract and internal governance retrospectively completed.
27/03/2020	IT Software	IT	Jeff Smyth (interim)	Interchange	£ 292,995	Low	Pending	PCR OJEU level	POL inherited the Galaxy system and support contracts from Royal Mail was part of, then descoped from compliant OJEU tender for Back Office in 2015
29/03/2020	IT Software	IT	Jeff Smyth (interim)	CSM Accent	£ 30,000	Low	Pending	Medium threshold	Part of the Galaxy solution for Swindon stocks, the future of Swindon has been under consideration for sometime and these licenses and support contracts have been rolled over year on year in the absence of a long term direction
29/03/2020	IT Software	IT	Jeff Smyth (interim)	JDW	£ 169,000	Low	Pending	Medium threshold	Part of the Galaxy solution for Swindon stocks, the future of Swindon has been under consideration for sometime and these licenses and support contracts have been rolled over year on year in the absence of a long term direction
29/03/2020	Media	Marketing & Brand	Emma Springham	Carat	£ 1,873,000	Low	In flight	PCR OJEU level	Contract extended to cover OJEU process time line which has been extended . Approved by Board March 2020
29/03/2020	Marketing	Marketing & Brand	Emma Springham	CACI	£ 392,380	Low	None	PCR OJEU level	No frameworks and no appetite in business for full OJEU. Limited other suppliers who have access to the market or simillar software. Software Reseller not an option. Approved by Board March 2020
29/03/2020	Banking Services	Operations & Supply Chain	Alisdair Cameron	RBS	£ -	Low	In flight	Lower threshold (PCR not applicable)	Covid19 crisis - cash services. Approved by Board March 2020
01/04/2020	Occupational Health	HR	Alisdair Cameron	Optima	£ 100,000	Low	In flight	PCR OJEU level	Interim extension to rectify CCS Framework legal drafting fault on GDPR. Approved by Board March 2020
29/04/2020	Goods for Resale	Retail & Franchise	Owen Woodley	Vow Retail Ltd	£ -	Low	In flight	Lower threshold (PCR not applicable)	Compliant standalone agreements not completed by 31/03/20. Approved by Board March 2020
29/04/2020	Goods for Resale	Retail & Franchise	Owen Woodley	Global Payments	£ 11,000,000	Low	In flight	PCR OJEU level	Interim extension to allow CCS tender process to be run. CCS Framework 9 months late to market on a rolling 2 month notice. Approved by Board March 2020
01/05/2020	Staff Uniforms & PPE	Operations & Supply Chain	Alisdair Cameron	SMI	£ 175,106	Low	None	Medium threshold	Covid19 crisis . Approved by Board March 2020
30/04/2020	Management consultancy	IT	Jeff Smyth (interim)	McKinsey	£ 400,000	Low	None	PCR OJEU level	Strategic review of Horizon system options. Approved at March 2020 Board
01/05/2020	Staff Uniforms & PPE	Operations & Supply Chain	Alisdair Cameron	Pink Office	£ 1,739,880	High	In flight	PCR OJEU level	Covid19 crisis . Approved by Board March 2020
01/05/2020	Staff Uniforms & PPE	Operations & Supply Chain	Alisdair Cameron	Fluid Branding	£ 195,450	Low	In flight	PCR OJEU level	Covid19 crisis . Approved by Board March 2020

Strictly Confidential

POL00423570

Date	Procurement Category	Function	GE Member	Supplier Name	Value/ Income	Risk Rating	Mitigation	Breach Type 1 - PCR Threshold	Reason for Breach
01/06/2020	Professional Services	HR	Lisa Cherry	Manchester Partners	£ 50,000.00	Medium	None	Medium threshold	Outplacement services for two senior leavers. Work awarded to Manchester Square without being tendered. No contract in place.
01/06/2020	Professional Services	Corporate Affairs & Comms	Ben Foat	KPMG	£ 107,000.00	Low	None	Medium threshold	Audit services to support GLO related review. Other firms conflicted out.
09/06/2020	Goods for Resale	Retail & Franchise	Owen Woodley	Vow	£ -	Low	In flight	Lower threshold (PCR not applicable)	Extended under a non-compliant Agreement (advertised under OJEU and extended beyond the advertised term)
25/06/2020	IT SaaS	Marketing & Brand	Emma Springham	Splash	£ 42,000.00	Low	Pending	Medium threshold	Reprocurement exercise was underway but due to Covid-19 and budget restraints this exercise had to be put on hold. Also require input from solution architect and workload has prevented this
25/06/2020	Banking Services	Retail & Franchise	Owen Woodley	Barclays	£ 2,700,000.00	Medium	Pending	PCR OJEU level	Contract extended with Barclays due to delays on digitisation project. A contract dispute led to a shorter term extension under the exemption and the final extension period now has an altered risk profile due to the delivery of the contracted programme of improvemnent.
25/06/2020	Banking Services	Retail & Franchise	Owen Woodley	Barclays	£ 500,000.00	Medium	Pending	PCR OJEU level	Service originally with Co-Op. they terminated the contract in order to exit cheque clearing market. Barclays stepped in to pick up service as very similar to cheque clearing.
20/06/2020	PR	Corporate Affairs & Comms	Richard Taylor	Cardew	£ 377,860.60	Low	Pending	PCR OJEU level	CEO / GE member appointment

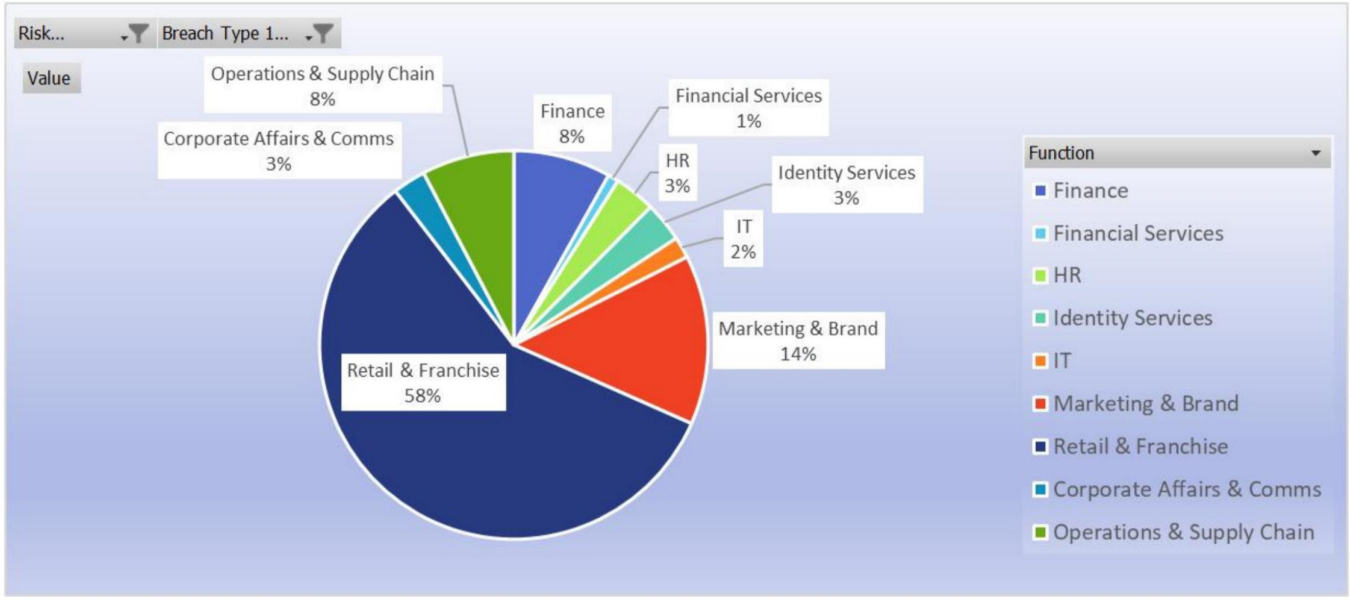
Strictly Confidential

POL00423570

Appendix C

Breakdown of Open Non Compliant Risk by £/Vol./Owner

Row Labels	Sum of Value/	
Alisdair Cameron	£	2,234,471.00
Nick Read	£	2,377,000.00
Owen Woodley	£	15,370,500.00
Lisa Cherry	£	850,000.00
Emma Springham	£	3,865,380.00
Amanda Jones (interim)	£	1,922,000.00
Richard Taylor	£	529,860.60
Jeff Smyth (interim)	£	491,995.00
Ben Foat	£	107,000.00
Grand Total	**£**	**27,748,206.60**



Strictly Confidential

POL00423570

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE REPORT

Title:	Policy Update	**Meeting Date:**	19th July 2020
Author:	Reena Chohan	**Sponsor:**	Jonathan Hill/Ben Foat

Input Sought:

Discussion:

The Committee is asked to review and approve the updated Policies and the 2020/2021 Modern Slavery Statement and endorse the proposed actions for the business to take these forward.

Executive Summary

This paper provides a summary of changes that have been made to the policies below as part of their annual review process for the RCC to consider.

Questions addressed in this paper?

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

Which policies were updated in this annual cycle review?

1. In this review cycle the following **8** policies were revised, reviewed and updated as per the annual review process.

Policy	Last Reviewed	Updates	GE Owner	Governance Approval Body
Modern Slavery Statement	July 2019	20/21 Statement records the progress made against previous commitments and commitments in place to continue those this financial year	Amanda Jones	RCC & ARC
Business Continuity Policy	July 2019	Changes to the CEO statement on the cover.	Jeff Smyth	RCC & ARC
Anti-Bribery and Corruption Policy	July 2019	Minor updates made – No Regulatory Changes	Ben Foat	RCC & ARC
Whistleblowing Policy	July 2019	Minor updates made – No Regulatory Changes	Ben Foat	RCC & ARC
Financial Crime Policy	Sept 2019	Legislation amendment and further enhancements made to the policy	Ben Foat	RCC & ARC

11

[Confidentiality Classification]

POL00423570

Anti -Money Laundering and Counter Terrorist Financing Policy	Sept 2019	Legislation amendment and further enhancements made to the policy	Ben Foat	RCC & ARC
Document Retention Policy	March 2018	Legislation and definition update.	Jeff Smyth	RCC & ARC
Procurement Policy	March 2014	Policy has substantially been rewritten to replace the previous policy dated March 2014	Alisdair Cameron	RCC & ARC

What updates were included and why?

2. A summary that identifies the changes and updates to the policies and statements have been added below:

Modern Slavery Statement:

3. The Post Office is compliant with the requirements of the Modern Slavery Act 2015 in terms of its legal obligations. It has made progress in defining what needs to be done across the business and is beginning the longer-term task of robust implementation. Post Office has prepared a new Statement for 2020/2021 in line with the Act. The Statement must be published on Post Office's website within 6 months of financial year end. There are measures in place to ensure it will be published online on or before 30th September 2020
4. The 2020/2021 statement records the progress we have made against those commitments and lists our commitments to tackle modern slavery across POL and POI for the financial year 2020/2021. The commitments were developed by the MSA Steering Group which includes representatives from Legal, Procurement, Risk, Employee Relations and Learning and Development. Good progress in 19/20 was seen across all of our commitments and in 20/21 our focus is more on maintaining and strengthening our MS procedures.

Business Continuity Policy:

5. The only changes being made to the current policy are in the CEO statement on the cover, the remainder of the Business Continuity Policy remains accurate and what we work to. The Policy is consistent with "ISO22301", which is the Business Continuity International Standard.

Anti-Bribery Corruption Policy:

6. Please refer to the annual review paper submitted. There have been no Regulatory changes to the policy, but minor amends have been made.

Whistleblowing Policy:

7. Please refer to the annual review paper submitted There have no Regulatory changes to the policy, but minor amends have been made in relation to the Whistleblowing Contact Details.

Financial Crime Policy:

8. Following review of legislation changes, incidents and assurance enhancements during 2019/20, amendments have been made to clarify terms and language and enhance some minimum control standards:

[Confidentiality Classification]

POL00423570

- Amended legislation section to incorporate that the 2017 MLRs have been amended by the Money Laundering and Terrorist Financing (amendment) regulations 2019
- Amended 'Electronic' Crime to 'Cybercrime' to reflect industry norm
- Updated associated policy references
- New corrective control:
  - Product Management must implement escalation procedures for when an incident is identified, so that the Financial Crime Team are made aware and if the product is outsourced to a third party, the third party is made aware. Product Management are responsible for addressing and overseeing any control failings to mitigate money laundering or terrorist financing risks.
- New preventative control:
  - Product and marketing managers must ensure that any product training, promotions or communications are in line with AML & CTF policy and processes
- Enhanced minimum control standards relating to product and service risk assessment process to reflect assessment enhancements introduced in 2019/20, including new Financial Crime Engagement Tool for initial product and service assessment.
- Minor amends to wording and definitions following Legal referral

9. With Regards to Financial Crime Policy Assurance and how the minimum required standards stated within the policy are being met, please refer to the Assurance Appendices submitted to the RCC reading room.

Anti-Money Laundering and Counter Terrorist Financing Policy:

10. Following review of legislation changes, incidents and assurance enhancements during 2019/20, amendments have been made to clarify terms and language and enhance some minimum control standards:

- Amended legislation section to incorporate that the 2017 MLRs have been amended by the Money Laundering and Terrorist Financing (amendment) regulations 2019
- New corrective control:
  - Product Management must implement escalation procedures for when an incident is identified, so that the Financial Crime Team are made aware and if the product is outsourced to a third party, the third party is made aware. Product Management are responsible for addressing and overseeing any control failings to mitigate money laundering or terrorist financing risks.
- New preventative control:
  - Product and marketing managers must ensure that any product training, promotions or communications are in line with AML & CTF policy and processes
- Enhanced minimum control standards relating to product and service risk assessment process to reflect assessment enhancements introduced in 2019/20, including new Financial Crime Engagement Tool for initial product and service assessment.
- Minor amends to wording and definitions following Legal referral

11. With Regards to AML/CTF Policy Assurance and how the minimum required standards stated within the policy are being met, please refer to the Assurance Appendices submitted to the RCC reading room.

[Confidentiality Classification]

POL00423570

Document Retention Policy:

12. The last annual review of the policy took place in March 2018 therefore the policy has been updated to reflect the new standardised format for Policies, given the various Document Retention Projects that have been in process the policy now reflects the changes that have come from these projects. There **have also been updates to the definition section of the** policy and the policy now reflects the current legislation.

Document Retention Policy:

13. The last annual review of the policy took place in March 2018 therefore the policy has been updated to reflect the new standardised format for Policies, given the various Document Retention Projects that have been in process the policy now reflects the changes that have come from these projects. There have also been updates to the definition section of the policy and the policy now reflects the current legislation.

Assurance

14. After a gap in time since there had been any resource in this area, Compliance is now working with Company Secretariat in re-establishing the key policy list for appropriate review and regular sign off as well as identifying any gaps.

15. Compliance will also be introducing a more robust process for future policy submissions and re-review by requiring policy owners to demonstrate how the minimum control standards stated within the policy are being met. As this process moves towards BAU we would propose to sample test some of these policies on a risk basis to review the policy standard and policy compliance.

Conclusion

We continue to work with Policy Owners and Company Secretariat to ensure we maintain our policy governance responsibilities.

[Confidentiality Classification]

POL00423570

POST OFFICE LIMITED RCC REPORT

Title:	Modern Slavery Act Statement	**Meeting Date:**	13/07/2020
Author:	James Scutt	**Sponsor:**	Andy Kingham

Input Sought: Decision

The RCC is asked to approve the 2020/2021 Statement and endorse the proposed actions POL will take forward in the 2020/2021 financial year.

Previous Governance Oversight

We consulted all members of the MSA Steering Group which comprises of representatives across functions including Legal, Procurement, Risk, Employee Relations and Learning and Development.

Executive Summary

The Modern Slavery Act 2015 (the Act) challenges slavery, domestic servitude, forced and compulsory labour and human trafficking. Post Office is required to produce an annual slavery and human trafficking statement (Statement) setting out what steps have been taken to ensure its business and supply chains are mitigating the risks of modern slavery. This paper attaches the third Statement which documents progress on our previous year's commitments and outlines the actions that we commit to take in the year ahead.

Overall the Post Office is compliant with the Modern Slavery Act 2015 in terms of its legal obligations. It has made good progress in defining what needs to be done across the business and has good activity and tracking in place.

- Post Office has prepared a new Statement for 2020/2021 in line with the Act. The Statement must be published on Post Office's website within 6 months of financial year end.
- The steering group has been meeting monthly, has made good progress and will continue to evolve and adapt going forward.
- Due to the lack of direct control over operations in this area, the highest level of risk continues to be within our Agency Network with several more areas identified where proximity of brand also poses a risk for Post Office (eg. When Post Office branding appears on retail packaging, sourced by one of its suppliers).
- Published company statements on modern slavery face scrutiny from the media, pressure groups and the public. As an organisation with a reputation of trust and a stated social purpose, we consider it important for Post Office to demonstrate a clear commitment to combating modern slavery. Civil society would expect the Post Office to be a champion in this area because of this trust legacy.

Actions for 2020/21:

- Deploy a supplier evaluation audit via our Procure-to-Pay system, using a risk based selection methodology, with the aim of auditing 10 suppliers from the highest risk categories.
- Produce a set of robust guidelines on how different parts of Post Office business should report suspicions of Modern Slavery and how these should be investigated.

Confidential

POL00423570

- Continue to raise awareness of Modern Slavery across Post Office supply chain and branch network in both directly managed and agency branches.
- Re-deploy specific, annual Modern Slavery awareness training to our field teams to enable them to robustly spot signs of Modern Slavery on an ongoing basis.

Questions addressed

1. Why do we need an updated Statement?
2. What are the key points to note about our Statement?
3. Is the Post Office compliant with the Act?

Report

Why do we need Modern Slavery Act Statement?

The requirement to publish a Statement applies to "commercial organisations" which (a) supply goods or services and (b) have a total turnover of not less than £36 million. It will therefore not apply directly to Postmasters if their annual turnover is less than £36 million. As Postmasters are part of the Post Office supply chain, Post Office must state what steps it has taken to ensure that it mitigates the risk of slavery and human trafficking in any of its supply chains or its business. Payzone has a turnover well below the threshold so is not legally required to produce a separate Modern SlaveryStatement. Our Modern Slavery Statement also covers Payzone, as a business owned by the Post Office.

Post Office is required under s.54 of the Act to produce an annual slavery and human trafficking statement listing the steps taken to ensure its business and supply chains are slavery free. This paper attaches the fourth Statement (Appendix 1) which records what steps we have taken in 2019/2020 and outlines the actions we commit to take in 2020/2021. The Statement must be approved by the Post Office Board and signed by a Director.

What are the key points to note about our updated Modern Slavery Act Statement?

Our 2020/2021 statement records the progress we have made against those commitments and lists our commitments to tackle modern slavery across POL and POI for the financial year 2020/2021. The commitments were developed by the MSA Steering Group which includes representatives from Legal, Procurement, Risk, Employee Relations and Learning and Development. Good progress in 19/20 was seen across all of our commitments and in 20/21 our focus is more on maintaining and strengthening our Modern Slavery procedures. The majority of the risk sits in the Retail Network.

Our commitments (in bold) and progress in 2019/20 were:

Implement a new IT system to track and monitor the on-boarding of new suppliers, ensuring a robust assessment and oversight of their ways of working and risk profile around Modern Slavery.

- As planned we went live with our Procure2Pay system. This changes the way goods and services are ordered, approved and receipted across Post Office. It also changes the way in which we manage and interact with our suppliers, improving our MS assessment and due diligence processes.

POL00423570

Review our supply base retrospectively by applying the focus of our new IT tracking system.

- Between Oct 2019 and March 2020 we phased a re-registration of 621 suppliers, which put them through our enhanced due diligence process which includes Modern Slavery.
- A confirmation of the Supplier Code of Conduct, which includes Modern Slavery, is required during on-boarding and is available publicly on our website.

Raise awareness of Modern Slavery across our existing suppliers where they are found to be lacking focus.

- A supplier evaluation audit was conducted with 3 of our major suppliers, Banner (our stationery supplier), Atalian Servest (cleaning) and Dimensions (uniforms), to test the methodology and feedback mechanism. This included feedback and improvement actions.
- During our re-registration process and enhanced Modern Slavery assessments, none of our suppliers were found to be lacking in focus.
- However, we have reiterated to all suppliers, during the re-registration process, their obligations in respect of Modern Slavery.

Continue to raise awareness of Modern Slavery across Post Office supply chain and branch network in both directly managed and agency branches.

- During our supplier re-registration process we have reiterated to all suppliers, their obligations to Modern Slavery.
- Across our branch network we re-issued our guidance on Modern Slavery awareness for Postmasters through our branch Network field teams and communication channels.
- For POL Employees, alongside our Modern Slavery Training, we issued guidance and comms around Anti-Slavery day, highlighting Government best practice to end modern slavery.
- For Postmasters we issued 2 clear comms in the year 2019/20; one highlighting Government best proactive and available resources and the second around "Dirty Money" and how this can result in Modern Slavery.
- Links to all three comms can be found in Appendix 3.

Deploy specific Modern Slavery awareness training to our field teams to enable them to robustly spot signs of Modern Slavery.

- We deployed specific online Modern Slavery training to educate our field team and made this mandatory to all team members. These teams are specifically in roles who actively support our branches.
- We achieved over 98% completion of the training by current employees and new joiners of these teams now receive the training as standard.
- We also surveyed colleagues who completed the Modern Slavery training and found that, after receiving a 93.5% response rate to the survey;
    - 97% of respondents agreed that they are aware of the signs of Modern Slavery
    - 81.7% agreed that they actively look for the signs of Modern Slavery during each branch visit.

POL00423570

- 87.4% of respondents were confident of the process to report potential Modern Slavery incidents.
- A full report on the survey results can be found in Appendix 3.

Review the guidance given to Postmasters to ensure alignment with wider business activity and network support teams.

- In association with the National Federation of Subpostmasters (NFSP) we have reviewed the guidance we give to our Postmasters which has been communicated as above.

POMS

Over the past 18mths, POMS have carried out due diligence and reviews on the following gold/silver suppliers but to date have found no material issues with the Suppliers' adherence to the MSA:

- BISL - Identified during review
- Cardif Pinnacle
  - Review started but postponed due to Covid-19, but found the MSA statement within their Group in the preparation and it was up to date
- CISL - Not required due to annual turnover level
- ERGO - Part of RFP last year. Group Statement identified
- Taurus - Part of RFP last year. Not required due to annual turnover level
- Webhelp - Identified during review
- Royal London - Identified during review

The one area we located a gap was for supplier our supplier "Reassured"

The following mitigating points to note:

- POMS were already aware of the gap and had an action in place
- This year was the first time Reassured had reached/exceeded the turnover level to require an MSA Statement.
- Bridgepoint have recently acquired the supplier and do have a modern slavery statement already

The action was identified in the Assurance Review for the MSA to be reviewed and for the statement to show in their next Business Report.

The vast majority of suppliers within the POMS Supply Chain do not fall within the remit of requiring an assurance review, but neither would many of these trigger the required MSA review and Statement due to the size of them.

For Post Office Group, the main areas of risk are highlighted as:

Public perception that where a Post Office fascia is in place that the facility is a Post Office and not an independent retailer that "includes" a Post Office service.

Risk by association that those working with a Post Office fascia but also operating other businesses, directly and indirectly associated with retail.

POL00423570

Challenging dialogue to have with consumers about trust and control of Postmasters if something goes wrong. Given the public perception is that the Post Office controls all places where there is a Post Office facia, stating in defence that: "We do not control them", "We did not know about this", "We have T&Cs that prohibit this", would not be good enough in the public domain, and there would be reputational damage.

Is the Post Office compliant with the Act?

Overall the PO is compliant with the legal obligations of the Modern Slavery Act.

To establish the level of monitoring and due diligence within the Post Office that would be expected by civil society and stand up to public scrutiny, continued focus and resource is required. Overall the Post Office is compliant with the legal obligations of the Modern Slavery Act 2015. It has made good progress within the business and delivered against its commitments made in year 2019/20.

Financial Impact

4. None

Risk Assessment, Mitigations & Legal Implications

A potential consequence of failing to show adequate progress on tackling modern slavery within the company statement is damage to reputation and brand.

Government guidance on the Modern Slavery Act and expectations from civil society is for companies to show year on year progress on how they are tackling the risks of modern slavery within their operations and supply chain.

Our annual statement therefore has to be more than just a tick-box exercise and must demonstrate a material commitment to tackling the potential risk of modern slavery within the organisation.

We are confident that the detail in our 2020/2021 statement recording our progress on last year and our proposed actions for the financial year 2020/2021 are appropriate. We will monitor developments, and keep the adequacy of the Statement under review.

11

Stakeholder Implications

5. None

Other Options Considered

6. None

Next Steps & Timelines

The Statement must be published on Post Office's website within 6 months of financial year end. (30th September 2020)

POL00423570

Appendix 1

1. Modern Slavery Statement 2020/2021

MODERN SLAVERY ACT TRANSPARENCY STATEMENT 2020/21

Post Office Limited (Post Office) & Post Office Management Services Limited (POMS).

This statement is made pursuant to section 54(1) of the Act. It sets out the steps taken by Post Office & POMS during year ending 31st March 2030 to mitigate the risks of modern slavery and human trafficking in its business and supply chains.

Post Office and POMS are committed to combating the risk of modern slavery or human trafficking in our supply chain and business operations. We are committed to taking appropriate steps to ensure that everyone who works for Post Office in any capacity, benefits from a working environment in which their fundamental rights and freedoms are respected.

This is the fourth statement in which we report on our efforts to mitigate the risks of modern slavery in line with the requirements of the Act. Our history has seen us focus on the rights and wellbeing of the people who work for Post Office and for our suppliers for many years. Our statement provides details of our policies, our approach and the actions we have taken in the 2019/20 financial year to strengthen our programme and commitment to respect and uphold people's fundamental rights and freedoms.

OUR BUSINESS AND SUPPLY CHAIN

Post Office is the UK's largest retail network and the largest financial services chain in the UK. We have provided services for more than 370 years and currently supply a range of essential products and services to communities' right across the UK.

Our UK Government mandate is to provide at least 11,500 Post Offices, some within certain geographical, demographic and social criteria that provide a unique operational challenge for Post Office compared to other wholly commercial retail or financial institutions. We are often at the heart of the local communities, some of which can be challenging environments to operate in.

Post Office directly controls around 1% of the Network of branches which consumers will generally recognise as the larger branches often situated in the centre of towns and cities across the UK. The remainder of the branches are managed on an agency basis by independent small retailers and shop owners operating Post Office services within their own store. Business owners may own more than one shop operating Post Office services and have a range of other non-connected business interests. We also have agent managed facilities within some larger high street commercial partners, who like the smaller independent retailers, provide their own trained and friendly staff to provide our Post Office services to consumers.

Banking services

Post Office banking services are provided in Post Office branches on behalf of the customers of UK banks.

Postmasters

Postmasters can operate one or more branches. As agents they have full control over how their branches within their retail premises are run on a daily basis. All those working in an agency Post Office branch are employed directly by the retailer. The Retailer is self-employed and typically takes on a Post Office as a valuable community service provided within their own retail business. Post Office has no direct control over the operation of these independent

POL00423570

SME businesses but does have the ability to influence and inform. Post Office aims to support Postmasters with their Post Office operations and influence their behaviours.

Commercial partners

A large proportion of the agency network is managed by commercial partners – corporate retail organisations with familiar fascia brands who themselves have a multiple number of high street stores.

Trade Unions

In our directly managed branch network, we work closely with the Communications Workers Union (CWU) and Unite (CMA) Communications Managers Association.

Third Party Suppliers

We also procure products and services from a range of managed suppliers, ranging from small and medium enterprises to large multinationals. Purchasing for our own managed Post Offices is controlled centrally by the Procurement team who also set the Supplier Relationship Management standards to ensure our teams maintain a consistent approach to supplier management.

OUR BELIEFS AND PRINCIPLES

Respect for the dignity of the individual and the importance of each individual's human rights form the basis of the behaviours we expect in every workplace and are communicated through our Code of Business Standards. We will not accept any form of discrimination, bullying or harassment. We require all our managers to implement policies designed to ensure equality of opportunity and inclusion for all Post Office employees.

OUR POLICIES

We operate a number of policies to ensure we are conducting business in an ethical and transparent manner. These include:

CODE OF BUSINESS STANDARDS

We have a Code of Business Standards which underpins everything we do. The Code is mandatory and extends to everyone directly employed by Post Office and is reviewed every 24 months. Although it is reviewed every 2 years, there are ad hoc changes undertaken when required, with all changes recorded in the policy on people hub.

It requires all of us to act ethically and comply with legal requirements at all times, putting our principles into practice in everything we do. The Code of Business Standards was updated during the 2018 financial year to include references to Modern Slavery.

WHISTLEBLOWING

We operate a Whistleblowing Policy so that all Post Office employees know how to raise concerns regarding wrongdoing or dangerous practices. The policy was updated during the 2019 financial year to include references to concerns about Modern Slavery.

There are a number of ways people can report any concerns regarding slavery or human trafficking within Post Office, by either contacting the Whistleblowing Officer or via our anonymous external confidential reporting service 'Speak Up' which is regularly communicated to all employees, suppliers and contractors. This is overseen by our General Counsel (Whistleblowing Officer). Every report submitted is assessed and investigated.

RECRUITMENT & ONBOARDING POLICY

POL00423570

Our recruitment and on-boarding policy for Post Office employees sets out the overarching principles and controls to be followed and applied to ensure that personnel resourcing is conducted in a fair, open and transparent manner, including conducting eligibility to work in the UK checks for all employees.

DUE DILLIGENCE PROCEDURES IN RELATION TO SLAVERY AND HUMAN TRAFFICKING IN OUR BUSINESS AND SUPPLY CHAIN.

Post Office/POMS employs solely within the UK.

Our recruitment procedures ensure that all prospective employees are legally entitled to work in the UK. All successful applicants must produce, on their first day, one of the following: their original passport, driving license or birth certificate. Additionally, to comply with the Asylum and Immigration Act 1996 requirements, if they are from a non-European Economic Area (EEA) country, evidence of a right to reside and work in the UK must be produced.

We carry out reasonable and practical due diligence in the sourcing of goods and services and ensuring that the Act's obligations form part of the procurement process. As part of this process we have conducted a review of the criteria used by Post Office to evaluate whether suppliers meet Post Office's minimum tendering requirements. We have also reviewed our standard form procurement contracts to ensure that they make explicit reference to the Act, as well as covering other areas of company information, policies and procedures. This enables the procurement team to assist Business Units to identify and assess any potential risks relating to the goods or services being procured.

IDENTIFYING, ASSESSING AND MANAGING RISK

WHERE ARE THE RISKS OF MODERN SLAVERY AT POST OFFICE/POMS

Post Office understands that our procurement of goods and services from third parties carry with it the risk of modern slavery and human trafficking.

We understand that a potential for risk of modern slavery sits within our agency network as there are a large number of people employed by independent retailers acting as Postmasters (including commercial partners) who are not direct employees of Post Office or POMS.

GOVERNANCE

We have a cross-functional steering group through which we develop and coordinate our approach to addressing modern slavery risks within our operations and supply chain. This group consists of expertise from the legal, procurement, compliance and operational functions in Post Office.

TRAINING

We provide annual Compliance Awareness Training to all our employees and postmasters, which is tailored to ensure an appropriate level of understanding of issues such as modern slavery and the Act's requirements.

WHAT DID WE DO THIS YEAR

Proposals from 2019/20 Statement	Progress on 2019/20 proposals
Implement a new IT system to track and monitor the on-boarding of new suppliers, ensuring a robust assessment and oversight of their ways of working and risk profile around Modern Slavery.	As planned we went live with our Procure2Pay system. This changes the way goods and services are ordered, approved and receipted across Post Office. It also changes the way in which we manage and interact with our suppliers, improving our Modern Slavery assessment and due diligence processes.

Confidential

POL00423570

Review our supply base retrospectively by applying the focus of our new IT tracking system.	Between Oct 2019 and March 2020 we phased a re-registration of 621 suppliers, which put them through our enhanced due diligence process which includes Modern Slavery. A confirmation of the Supplier Code of Conduct, which includes Modern Slavery, is required during on-boarding and is available on our website at http://corporate.postoffice.co.uk/our-suppliers
Raise awareness of Modern Slavery across our existing suppliers where they are found to be lacking focus.	A supplier evaluation audit was conducted with 3 of our major suppliers to test the methodology and feedback mechanism. This included feedback and improvement actions. During our re-registration process and enhanced Modern Slavery assessments, none of our suppliers were found to be lacking in focus. However, we have reiterated to all suppliers, during the re-registration process of their obligations to Modern Slavery.
Continue to raise awareness of Modern Slavery across Post Office supply chain and branch network in both directly managed and agency branches.	During our supplier re-registration process we have reiterated to all suppliers, their obligations to Modern Slavery. Across our branch network we re-issued our guidance on Modern Slavery awareness for Postmasters through our branch Network field teams and communication channels.
Deploy specific Modern Slavery awareness training to our field teams to enable them to robustly spot signs of Modern Slavery.	We deployed specific online Modern Slavery training to educate our field team and made this mandatory to all team members. These teams are specifically in roles who actively support our branches. We achieved over 98% completion of the training by current employees and new joiners of these teams now receive the training as standard. We surveyed colleagues who completed the Modern Slavery training and found that, after receiving a 93.5% response rate, 97% of respondents agreed that they are aware of the signs of Modern Slavery and 81.7% agreed that they actively look for the signs of Modern Slavery during each branch visit. 87.4% of respondents were confident of the process to report potential Modern Slavery incidents.
Review the guidance given to Postmasters to ensure alignment with wider business activity and network support teams.	In association with the National Federation of Subpostmasters (NFSP) we have reviewed the guidance we give to our Postmasters which has been communicated as above.

POL00423570

WHAT COMMITMENTS ARE WE MAKING TO TACKLE MODERN SLAVERY IN THE YEAR AHEAD

As part of our initiative to identify and mitigate risk throughout 2020/21 we are committed to:

- Deploy a supplier evaluation audit via our Procure-to-Pay system, using a risk based selection methodology, with the aim of auditing 10 suppliers from the highest risk categories.
- Produce a set of robust guidelines on how different parts of Post Office business should report suspicions of Modern Slavery and how these should be investigated.
- Continue to raise awareness of Modern Slavery across Post Office supply chain and branch network in both directly managed and agency branches.
- Re-deploy specific, annual Modern Slavery awareness training to our field teams to enable them to robustly spot signs of Modern Slavery on an ongoing basis.

REMEDIATION PROCESSES

If you have any concerns about the issues raised in this statement or if you think you have identified signs of Modern Slavery then please contact us on the below contacts:

Post Office's Whistleblowing Officer: whistleblowing GRO or by telephone on: GRO

The Government's Modern Slavery Helpline on GRO

We encourage any individual who has concerns about unethical behaviour in any part of our business or operations to speak up and to do so without fear of retaliation. We will review all instances of non-compliance, on a case-by-case basis and will implement appropriate remedial action.

REVIEW

This statement shall be reviewed and published annually

Confidential

POL00423570

Appendix 2

Supplier code of conduct

Please see attached file.

Appendix 3

Modern Slavery questionnaire

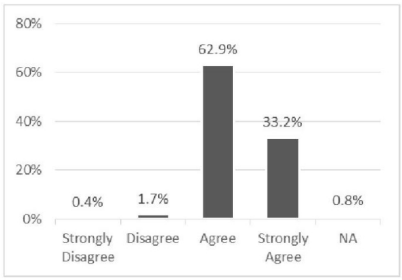
A summary of the responses from PO employees after completing the Modern Slavery training.

230 responses from 246 expected (93.5% response rate)

- Anyone who has not completed will find this remaining in their SFL as overdue

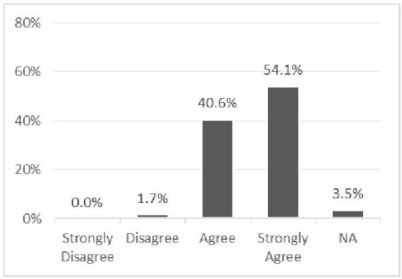
I understand the Modern Slavery Act sufficiently to meet both the Post Office and my legal requirements.

- Strongly Disagree 0.4%
- Disagree 1.7%
- **Agree 62.9%**
- **Strongly Agree 33.2%**
- NA 0.8%



I think Modern Slavery is a serious concern.

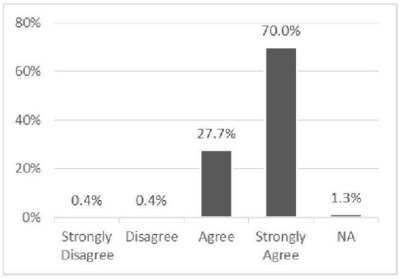
- Strongly Disagree 0%
- Disagree 1.7%
- **Agree 40.6%**
- **Strongly Agree 54.1%**
- NA 3.5%



11

I would never turn a 'blind eye' to a suspicion of a Modern Slavery incident.

- Strongly Disagree 0.4%
- Disagree 0.4%
- **Agree 27.7%**
- **Strongly Agree 70.0%**
- NA 1.3%

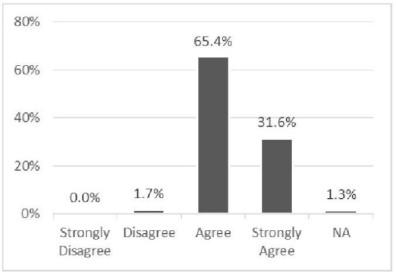


Confidential

POL00423570

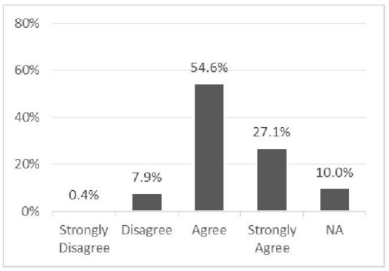
I am aware of the signs of Modern Slavery.

- Strongly Disagree 0%
- Disagree 1.7%
- **Agree 65.4%**
- **Strongly Agree 31.6%**
- NA 1.3%



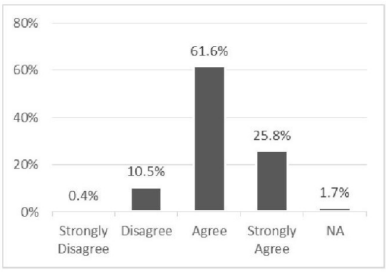
I look for the signs of Modern Slavery during each branch visit.

- Strongly Disagree 0.4%
- Disagree 7.9%
- **Agree 54.6%**
- **Strongly Agree 27.1%**
- NA 10.0%



I my confident of the process to report potential Modern Slavery incidents.

- Strongly Disagree 0.4%
- Disagree 10.5%
- **Agree 61.6%**
- **Strongly Agree 25.8%**
- NA 1.7%



Appendix 4

Modern Slavery Comms

Three comms pieces issues in year 2019/20 covering Modern Slavery:

For POL employees

- https://poluk.sharepoint.com/sites/thehub/SitePages/Anti-slavery-Day-%E2%80%93-Post-Office%E2%80%99s-commitment-to-tackling-modern-slavery.aspx

For Postmasters

- https://www.onepostoffice.co.uk/secure/help-me-do-my-job/branch-focus/compliance/anti-slavery-day-post-office-s-commitment-to-tackling-modern-slavery/
- https://www.onepostoffice.co.uk/secure/help-me-do-my-job/branch-focus/security/where-dirty-money-comes-from/

11

Confidential

POL00423570

Post Office - Supplier Code of Conduct

We are the Post Office and there is no-one like us. From our travel and financial services, passports to postage, the Post Office network is serving communities across the UK. We have a network of more than 11,500 branches across the UK and every one of our branches is at the heart of its community.

Maintaining our reputation for ethical business integrity is absolutely vital and we need to make sure that all of our suppliers work to our values. This short supplier code provides an explanation of the standards of behaviour that we expect when working for Post Office in support of our values **Care, Challenge** and **Commit**.

The requirements for you as a supplier are clear - comply with legislation, follow Post Office policy and procedures (including this Code), and if ever you are asked to do anything which sits outside of these parameters then please do tell us about it.

Responsibilities

Suppliers must comply with any terms and conditions that they have agreed with Post Office, and must ensure that all activities are undertaken safely, with no detriment to the well-being of your employees, our staff or the public. All work must be undertaken with care for the environment.

You must ensure that your employees are aware of their duties and are trained and competent to undertake the tasks they are employed for, and suitably supervised where required. Suppliers should be mindful that the activities of their organisation and staff can impact not only their own reputation, but that of the Post Office too. We expect suppliers at all times to ensure that the values and the good name of the Post Office are upheld.

This Supplier Code of Conduct is not a substitute for entering into a written contract with Post Office. It is an advisory document to explain our expectations of responsible behaviour from our suppliers, and to ensure that our standards are understood.

Bribery and Corruption

Suppliers must ensure that bribery or corruption are not tolerated and strict rules for the offering or acceptance of gifts and hospitality are adhered to. You must not offer bribes, kick-backs, gifts or hospitality to a Post Office employee in an attempt to gain a commercial advantage, or to any other employee or organisation to secure an advantage on behalf of Post Office, or to any other employee or organisation to secure an advantage on behalf of Post Office. Any conflicts of interest (for example a family connection between a supplier and the Post Office) need to be disclosed immediately.

Tax Evasion and the Facilitation of Tax Evasion

Tax evasion and the facilitation of tax evasion are both a criminal offence that can be punishable with imprisonment and /or unlimited financial penalties depending on the seriousness of the offence. Suppliers must not ask or encourage a Post Office employee to engage in a relationship which could result in the reduction or diversion of any taxes from any collecting authority. Please read our GUIDANCE – Criminal Finances Act 2017 document on our website http://corporate.postoffice.co.uk/our-suppliers.

POL00423570

Human Rights

Suppliers are expected to adhere to all Human Rights legislation. Specifically, this will include no child or forced labour, threat of violence, harassment, intimidation, debt bondage, bonded labour, or compulsory overtime when providing services. Disciplinary and grievance procedures should be fair and transparent, and include the right of appeal.

Employees should be allowed to terminate employment on reasonable notice, enjoy freedom of movement, incur no hiring fees, and be paid and work hours in accordance with national regulations including applicable minimum wage legislation. Where applicable, suppliers are expected to publish their annual statement on Human Trafficking and Modern Slavery in accordance with the Modern Slavery Act 2015.

Non-Discrimination

Suppliers are expected to practice a diversity and equality agenda in line with the Post Office values - with no discrimination on race, religion and belief, disability, gender reassignment, sexual orientation, age, pregnancy /maternity or marriage and civil partnership.

Freedom of Association

Suppliers should respect the rights of workers to associate or not to associate with any group, as permitted by and in accordance with all applicable local and national laws and freedom of association and collective bargaining. Suppliers shall not interfere with or discriminate against workers choosing to belong to them. Where the right to freedom of association and collective bargaining is restricted under national law, suppliers should facilitate, not hinder, alternative means of independent and free association and bargaining.

Confidentiality

Suppliers must ensure that they respect the confidentiality of Post Office information. They must not share any confidential information unless specifically authorised to do so by Post Office, and only process Post Office Personal Data in accordance with Post Office's instructions and as required by law.

Suppliers should notify the Post Office promptly (within 24 hours) if it becomes aware of any actual, suspected or threatened unauthorised exposure, access, disclosure, Processing, use, communication, deletion, revision, reproduction or transmission of any component of Post Office Personal Data, unauthorised access or attempted access or apparent attempted access (physical or otherwise) to Post Office Personal Data or any loss of, damage to, corruption of or destruction of Post Office Personal Data (Security Incident).

The Post Office is subject to the requirements of the Freedom of Information Act (FOIA) and the Environmental Information Regulations and suppliers will be required to assist and cooperate with Post Office to enable us to comply with our information disclosure obligations.

Insurance

Suppliers must maintain policies of insurance to provide a level of cover sufficient for the work that they intend to provide, and relevant for their own legal jurisdiction and any other jurisdictions they intend to work in with Post Office. This should include all risks that may be incurred by the supplier if any Purchase Order is issued, be it electronically, verbally, written or expressed. This includes cover for death or personal injury, loss of or damage to property, and professional advice. Levels of insurance shall be set within any contract, where no contract has be issued then insurance payable will be unlimited.

POL00423570

No purchase order, no payment

We want our suppliers to be paid in a timely manner for the work they do in supplying Post Office with the important goods and services. Our standard terms are 30 days from receipt of a valid and accurate invoice entry onto our systems. To achieve this, we require the cooperation and assistance of suppliers to ensure that we have an efficient and controlled payment process. This includes a "No purchase order, no payment" policy.

This means that any Post Office employee placing an order with any of our suppliers must provide a valid purchase order (PO) number, and which must be quoted on all supplier invoices. Any request to change an order from a Post Office employee must be supported with a revised supplier quotation and an amended purchase order (PO) document from the Post Office. Suppliers should note that requests to change the goods or services ordered should not be accepted without this evidence.

Invoices not showing a valid PO number will be returned to the supplier for evidence of a PO, which may result in delayed payment. A PO number demonstrates to Post Office that the goods/services have been authorised by the business.

Supplier Audits

We will conduct audits of our suppliers that will look at all aspects of behaviour and legislative compliance. We will focus specifically on:

Modern Slavery - Where we would expect all suppliers to have taken steps within their organisation to:

- ensure all UK workers receive minimum wage and robust immigration checks
- map supply chains to identify where there is highest risk and exposure to modern slavery
- undertake site inspections
- provide training to employees and local suppliers on modern slavery risks and compliance
- review supplier contracts to include obligations to comply with the Modern Slavery Act 2015
- prepare a statement outlining the steps you are taking to tackle modern slavery and publish it if required to do so by the Act.

Anti-Bribery and Corruption – Where we would expect all suppliers to have taken steps to:

- have an Anti-Bribery and Corruption policy in place
- give employees awareness training in Anti-Bribery and Corruption
- operate a hospitality register to track offers and invitations
- have a method to enable staff to raise concerns if they have any suspicions.

What do I do if something isn't right?

At the Post Office, we apply a zero tolerance for unsafe working practices, discrimination, fraud, bribery, tax evasion and the facilitation of tax evasion or corruption. We have a whistleblowing policy and we encourage our staff and suppliers to raise concerns with us. If you are ever asked to be involved in anything unethical or illegal then you must do the right thing – please "speak up". The same applies if you or your colleagues are treated unfairly while working for the Post Office. There are two ways in which suppliers can report a concern:

1. By contacting their Procurement contact or Vendor Manager or
2. By contacting the Grapevine confidential reporting service on GRO

POL00423570

Please sign, scan and return to your Post Office contact:

Supplier Code of Conduct

Declaration

Do you have any declared interests, or are aware of a connection in any way to a Post Office employee? E.g.: Family relationships, personal friendships, business interests.

Acceptance

I/We acknowledge receipt of a copy of the "Supplier Code of Conduct" and "Guidance - Criminal Finances Act 2017", and agree to observe the expected standards specified therein whilst carrying out work on behalf of the Post Office.

I/We will bring these rules to the attention of my/our employees and any further suppliers or sub-contractors to whom I provide work on contracts for the Post Office, and I/we will be responsible for ensuring their strict adherence.

SIGNED for and on behalf of (Supplier)
SIGNATURE(S)

PRINT NAME(S)

POSITION(S)

COMPANY

COMPANY REG. NO

DATE

POL00423570

POST OFFICE LIMITED RISK & COMPLIANCE COMMITTEE REPORT

Title:	**Annual Anti Bribery and Corruption Report**	**Meeting Date:**	13th July 2020
Author:	**Sally Smith**	**Sponsor:**	Ben Foat

Input Sought: Discussion

The committee is asked to review the contents of this report, approve the actions from the ABC risk assessment, updated ABC Policy, re-confirm the Corporate website statement and consider whether any further actions should be taken to improve ABC controls or gifts and hospitality reporting.

Previous Governance Oversight

The last annual ABC report and Policy amends were approved in July 2019

Executive Summary

Overall the ABC risk assessment demonstrated that control strengths have improved since the last review and did not identify any areas of material concern. The inherent risks identified are not unique to Post Office Limited and are expected as part of conducting business. The overall residual risk, although outside of risk appetite, is considered low to moderate.

The assessment has identified risk areas that require mitigation, and the full report outlines how Post Office can increase the control strength and reduce the residual risk score, and ultimately reduce its exposure to the risk of bribery and corruption. An action plan is being produced, and implementation of the recommendations, would bring the residual risk within Post Office risk appetite.

There are no material changes to the ABC policy, nor any changes to legislation since the last review.

Formal monitoring of compliance with the ABC policy minimum controls standards is in place, providing assurance that Post Office is complying with its ABC policy. Where failings are identified, these are escalated to the RCC or ARC as appropriate with recommendations to address.

The reporting and approval of gifts and hospitality has continued to improve, albeit some common errors do recur and it is likely that there is still under-reporting.

POL00423570

Questions addressed

1. What issues have been highlighted by the ABC risk assessment and annual review of Gifts & Hospitality?
2. What actions need to be undertaken to address any issues?
3. What changes to the Policy do we propose and why?
4. What are the implications of these changes?

Report

Summary of ABC activities 2019-20:

5. There has been no change to regulation or legislation in 2019/20, and no significant UK-based bribery and corruption cases.
6. Annual training was delivered to all employees in September 2019, and included a number of animations to re-inforce Gifts & Hospitality reporting requirements. On-going completion of training is tracked on a monthly basis, including new joiners.
7. Quarterly reporting is provided to all GE members summarising overall Post Office Gifts & Hospitality reporting and highlighting any breaches or concerns for each GE member.
8. Following a number of amendments during the year to the Gifts & Hospitality reporting tool and guidelines, there has been a marked improvement in reporting accuracy. The Gifts & Hospitality tool was completely re-built and re-launched in April 2020, with improved workflows and reporting to help drive further conformance. Some IT issues have been identified, and some modifications are currently being developed by IT to resolve. There has been minimal reporting during Covid lockdown.
9. Eight communications were issued relating to ABC and Gifts and Hospitality reporting.
10. The Corporate website ABC statement has been reviewed, but no changes are recommended (see Appendix A for current statement).
11. Activity to provide quarterly assurance of compliance with policy minimum control standards has further matured during the year, and the most up to date assessment (Q1 2020/21) can be found in Appendix D.

Annual Policy review:

12. Following the ABC risk assessment, minor amends have been made to clarify and enhance some minimum control standards:
    - Added a definition for internal bribery risks, and a minimum control standard
    - Clarified definitions relating to 'Group', 'staff' and 'employee'
    - Clarified sponsorship and charity definitions and controls
    - Added minimum control standards relating to procurement and agent on-boarding
    - Clarified some controls relating to gifts & hospitality approval

Annual Gifts & Hospitality review

15. Analysis of the 2019/20 Gifts & Hospitality Register has highlighted a slight increase in the volume of reports and the overall quality of submissions compared to 2018/19 (please

POL00423570

see Appendix B&C), although it is likely that some gifts and hospitality are still not being reported by recipients/offerors:

- In 2018/19 there were 47 gift reports totalling £4,918.64 and 187 hospitality reports totalling £38,703.54
- In 2019/20 there were 38 gift reports totalling £2,299.47 and 234 hospitality reports totalling £32,241.84

16. In the reporting period the following common breaches were identified:

- Further instances of employees accepting gifts of cash or cash equivalent (e.g. gift cards) from external third parties, some of which were approved by line management. In all instances the breaches were raised with line management, the cash returned and all employees in their area reminded of the policy requirements.
- Late retrospective submissions/approval after the event continue to be the most common issues. The new G&H Reporting Tool, is expected to help reduce these issues due to improved information capturing and accessibility of the tool.

17. A review of the external companies that have offered hospitality to Post Office in 2019/20 has not identified any significant issues, and the top 7 are detailed below:

External Third Party	Employee Response	Report Volume	Volume of People	Total Value
Capita Travel and Events	Accepted	3	3	£179.45
	Declined	2	2	£1,000.00
	Total	**5**	**5**	**£1,179.45**
MoneyGram	Accepted	12	9	£1,185.00
	Declined	0	0	£0.00
	Total	**12**	**11**	**£1,185.00**
Pinsent Masons	Accepted	4	13	£1,093.00
	Declined	0	0	£0.00
	Total	**4**	**13**	**£1,093.00**
Trethowans LLP	Accepted	1	2	£990.00
	Declined	0	0	£0.00
	Total	**1**	**2**	**£990.00**
Webhelp	Accepted	0	0	£0.00
	Declined	1	1	£800.00
	Total	**1**	**1**	**£800.00**
FRES	Accepted	6	7	£688.00
	Declined	0	0	£0.00
	Total	**6**	**7**	**£688.00**
Fujitsu	Accepted	3	11	£510.00
	Declined	1	1	£150.00
	Total	**4**	**12**	**£660.00**

Note: In 2018/19 Womble Bond Dickinson were the largest donor with 5 offers totalling £4,870, in 2019/20, POL employees received 1 offer, totalling £40.

Risk Assessment, Mitigations & Legal Implications

13. In quarter one 2020/21, an Anti-Bribery & Corruption (ABC) assessment of Post Office Limited was undertaken (a full copy of the report and recommendations is in the Reading

POL00423570

Room). This was the first complete assessment undertaken since the review completed in 2017/18 by Thistle Initiatives.

14. The overall control strength has seen a positive increase, and this is due to improvements in the following key areas

- POL has new Articles of Association for all Group Companies and a framework document signed with BEIS and its shareholder representative, UKGI. The document sets out parameters within which Post Office is expected to operate, and subsequently there is more involvement from Government in decision making, reducing the risk of bribery.
- The Procurement process, both within and outside of the scope of Procurement Contract Regulations (PCR), has improved following the implementation of a new Contract Execution Policy, the 'Source to Settle' project, and a Supplier Audit Questionnaire for due diligence on existing suppliers. In addition, since the last assessment the business has matured its approach to the approval and archiving of contracts.
- The annual ABC training has been matured and training now includes animations to improve engagement. Greater attention has also been given to political donations and sponsorship.
- The Financial Crime Policy Assurance Framework to measure the effectiveness of the minimum control standards in the ABC Policy on a quarterly basis has been implemented since the last review. If a substantial or sudden drop in effectiveness is identified, this is escalated to the MLRO, and where appropriate reported to the RCC and ARC. A project is also underway to identify how the existing controls can be improved.

15. An action plan is being drawn up for the recommendations from the review, which if implemented, will bring the residual risk within risk appetite:

- In line with the Contract Management Framework the Legal team are developing, ensure signed copies of all contracts are held, these are in date and they contain the appropriate bribery clauses. Additionally, there are variations of agent contracts, which are being reviewed to ensure relevant ABC clauses are in place.
- Implement formal assurance monitoring procedures to ensure that existing suppliers have policies and procedures which are equivalent to Post Office.
- In line with the Compliance culture strategy under development, general adherence to group policies needs to improve, including regular certification from managers.
- Continue to raise awareness of Gifts & Hospitality policies and procedures and monitor expense reporting against reports made on the G&H tool to identify breaches in policy.
- The People and Policy Compliance Manager needs to work with policy owners to ensure policies are up to date and adhered to.
- Latest versions of all policies, procedures and codes of conduct, should be up to date and readily available for all employees, with previous versions removed.
- Publish a statement concerning charitable donations, as well as a formal approval process for employees wishing to donate to charities on behalf of Post Office.
- Implement a process to ensure any relevant employee's affiliation to a chosen charity has been identified for a conflict of interest, with each being considered on a case by case basis.
- Publish a statement concerning sponsorships, as well as a formal approval process for employees seeking approval from GE to accept sponsorship from a third party.

POL00423570

- Publish a statement concerning the award or acceptance of grants to both agent operators and employees, and ensure there are clear guidelines and controls surrounding approval.

Stakeholder Implications

16. No material changes are required to comply with the updated Policy.
17. The Financial Crime Team are working with the Head of Corporate Responsibility & Social Impact to improve processes and controls around sponsorship and charitable donations.
18. The Compliance team will work with stakeholders across the business to improve first line compliance with the ABC policy requirements as part of the overall Compliance strategy work.

Next Steps & Timelines

19. The Financial Crime Team will pursue and oversee the action plan to remediate the residual risks identified in the ABC risk assessment with relevant stakeholders during the rest of 2020/21.
20. Progress will be reported via Compliance reporting to the RCC and ARC.
21. The ABC training content is being updated and will be delivered to all employees in September 2020. On-going communication and awareness will be delivered throughout 2020/21.

Sally Smith
MLRO & Head of Financial Crime
25th June 2020

POL00423570

GROUP POLICIES

Anti-Bribery and Corruption Policy

Version – V4.2

11

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

POL00423570

1. Overview 3
1.1. Introduction by the Policy Owner 3
1.2. Purpose 3
1.3. Core Principles 3
1.4. Application 4
1.5. Types of Bribery and Corruption Risk 4
1.6. Legislation 5
1.7. FCA Rules 6
2. Risk Appetite and Minimum Control Standards 7
2.1. Risk Appetite 7
2.2. Policy Framework 7
2.3. Who Must Comply? 8
2.4. Gifts and Hospitality Tool 8
2.5. Minimum Control Standards 9
3. Definitions 1916
3.1. Definitions 1916
4. Where to go for help 2017
4.1. Additional Policies 2017
4.2. How to raise a concern 2017
4.3. Who to contact for more information 2017
5. Governance 2118
5.1. Governance Responsibilities 2118
6. Control 2219
6.1. Policy Version 2219
6.2. Policy Approval 2219
Company Details 2219

11

POL00423570

1. Overview

1.1. Introduction by the Policy Owner

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

1.2. Purpose

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

Commented [SS1]: Definition of employee and staff amended following Legal review – see footnote

1.3. Core Principles

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

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

- The Group is committed to and oversees the implementation of a Policy of zero tolerance, recognising that bribery is contrary to fundamental values of integrity, transparency and accountability and undermines the Group's effectiveness;
- Post Office has devised a robust Policy and associated procedures (set out in this document) which are proportionate to the risks and complexity of the Group;
- A bribery risk assessment is an integral part of our Group's overall and ongoing risk management process;
- Post Office must assess the risk associated with entering into joint ventures, partnerships or contracting arrangements with other entities and must carry out periodic due diligence based on that risk assessment. This includes ensuring that these organisations have policies and procedures which are equivalent to the Group's own procedures;
- The Group undertakes a training and awareness program to ensure employees are aware of the potential risks, how bribery might affect them, what they should do if

11

[1] In this Policy "Post Office" and "Group" mean Post Office Limited and any wholly owned subsidiary that formally adopts this policy
~~In this Policy "Post Office" and "Group" mean Post Office Limited and Post Office Management Services Limited.~~

[2] In this Policy "employee" and "staff" means all persons working for the Group or on our behalf in any capacity (other than Postmasters or their assistants), including employees at all levels, directors, officers, agency workers, seconded workers, volunteers, interns, contractors, external consultants, third-party representatives and business partners, sponsors, or any other person associated with us, wherever located~~In this Policy "employee" means permanent staff, temporary including agency staff, contractors, consultants and anyone else working for or on behalf of Post Office.~~

POL00423570

they are offered a bribe, and the consequences should they be found to have made or received a bribe;

- The interests of Policyholders and other stakeholders are protected by ensuring that excessive powers are not delegated to individuals;
- Decisions taken by management are consistent with the Group's strategic objectives and risk appetite, which are approved by the Board;
- Appropriate conduct is demonstrated in executing the requirements contained within the Policy;
- Every member of staff is responsible for understanding and managing the risk they take on behalf of the Group and for ensuring that they act within accordance to them;
- All employees are required to comply with Group Policies.

1.4. Application

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

In exceptional circumstances, where risk sits outside of the Group's accepted Risk Appetite a Risk Exception can be granted. Further information in relation to the risk exception process, together with a template can be found here.

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

For definitions please see section 3.1.

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

1.5. Types of Bribery and Corruption Risk

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

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

Commented [ML2]: Added to include sponsorships offered by third parties to the Group

11

POL00423570

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

~~3.~~4. **Internal bribery** – Post Office employees offering, requesting or receiving something of value from another employee in order to carry out their roles improperly or induce another employee to perform their roles improperly.

Commented [ML3]: Including internal bribery as a risk as we don't call this out, and our 2020 ABC risk assessment recommended to include internal bribery in this policy.

~~4.~~5. **Inducement Risks -** Post Office must take reasonable steps to ensure that it, and any person acting on its behalf, does not:

- Offer, give, solicit or accept an inducement; or
- Direct or refer any actual or potential business in relation to another person on its own initiative or on the instructions of an associate; if it is likely to conflict to a material extent with any duty that Post Office Management Services owes to its customers in connection with an insurance mediation activity or any duty which such a recipient firm owes to its customers in connection with an insurance mediation activity.

~~5.~~6. **Gifts & Hospitality** –The offer of Gifts & Hospitality by or to third parties represents a clear risk of inducement or facilitation and Post Office therefore has clearly defined minimum control standards and procedures for reporting and approving Gifts & Hospitality (both received and offered). Appendix A sets out the specific policy requirements and details of the process to be followed can be found on the Gifts & Hospitality reporting homepage here.

1.6. Legislation

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

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

Under the Bribery Act, it is an offence to:

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

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

11

POL00423570

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

The Bribery Act has extra-territorial effect which means that the actions of Post Office or a third party operating on our behalf outside of the UK may fall within the scope of the Act. In the context of Post Office, this could apply in scenarios such as where a Post Office contractor or supplier resides outside the UK. The Criminal Finances Act also includes a 'failure to prevent' (strict liability) offence on the Group, where failure to prevent criminal facilitation of a tax evasion offence, by a taxpayer, takes place and there are no reasonable procedures put in place to prevent such facilitation, or it cannot show that these procedures would have been unreasonable.

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

1.7. FCA Rules

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

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

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

POL00423570

2. Risk Appetite and Minimum Control Standards

2.1. Risk Appetite

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

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

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

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

2.2. Policy Framework

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

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

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

Commented [ML4]: Inclusion of agency network to cover bribery during on boarding process

11

[4] The Risk appetite was agreed by the Groups Board January 2015
[5] For more information in relation to Risk Exception waivers please see section 1.4

POL00423570

2.3. Who Must Comply?

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

Commented [ML5]: Changed to match the AML Policy wording.

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

~~All Post Office employees are required to report any knowledge or suspicions in relation to Bribery or Corruption to Grapevine. As such all business units are required to have a process in place for reporting Bribery or Corruption incidents to Grapevine by telephone on 0345 603 4003. For more information in relation to reporting knowledge or suspicions please see section 4.2.~~

Commented [ML6]: Paragraph deleted as deemed duplication of above.

2.4. Gifts and Hospitality Tool

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

The Gifts and Hospitality Tool can be found here.

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

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

11

POL00423570

2.5. Minimum Control Standards

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

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

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
Appointment and Activities of Consultants and Contractors	Failure to ensure that Consultants and Contractors comply with the Group's anti-bribery and corruption policy may lead to criminal prosecution and damage to the Post Office brand or reputation.	Preventative Control: Our contracts require Consultants and Contractors to comply with the Group's anti-bribery and corruption policy. A clause is included within Consultants and Contractors contracts requiring them to comply with the Group's anti-bribery and corruption policy. A Procurement Policy is maintained ~~exists~~ and training is provided to relevant staff. ~~is updated annually~~	Procurement Procurement	Ongoing where required Ongoing
Agent on-boarding	A Retail business or proprietor ~~—~~engages in bribery, such as offering gifts or hospitality or even a direct bribe to be considered favourably in the decision	The Group has a documented on boarding process for agent and branch selection and on boarding process which is regularly reviewed and all relevant staff are trained.	Agent On-boarding	Ongoing

Commented [ML7]: Inserted as one of ABC risk assessment recommendations is that the this policy is updated.

POL00423570

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
	making process for branch on boarding			
Charity Donations and Sponsorship	Insufficient controls may lead to the donation of a benefit or money to an unregistered charity, a registered charity or Good Cause Organisation that uses the donation to fund financial crime or bribery, or the acceptance of a donation by Post Office which could be interpreted as bribery and result in reputational damage.	Preventative Control: Where the Group, a team or an individual has selected a particular charity to support, they are required to validate that charity against the Charity Commissions website. More information can be found here.	All employees	Ongoing
		Where a supplier or third party requests that Post Office makes a charitable donation, or offers to make a donation to Post Office, Post Office ensures that the donation is not linked to any business or services provided to or by that supplier or third party.	All employees	Ongoing
		Any donations or sponsorship (cash or otherwise) ~~should~~ must be approved by the relevant GE member to ensure appropriateness.	GE are responsible for approval of donations and sponsorship	Ongoing
		~~and~~ For any donations or sponsorship, to or from Post Office, the details must be recorded on the central donations register.	The Financial Crime team maintain the donations register	Ongoing
		Post Office has a Group wide training programme to ensure		Ongoing

Commented [ML8]: Based on ABC RA recommendations, there isn't an existing MCS to mitigate this risk.

Commented [ML9]: Broadening the definition of charitable donations to include benefits, as well as money.

Commented [ML10]: A registered charity could be engaged in financial crime and referring to 'good causes' as not all are registered charities.

Commented [ML11]: In the ABC training we state "Line Manager and General Executive approval is also required, to confirm whether the charitable donation is appropriate"

POL00423570

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
		that all customer facing (branch) staff, back office staff and contractors receive adequate training. Staff and contractors are required to complete training within 30 days of joining Post Office and annually. ~~Outsource providers, clients & suppliers must maintain records to evidence that staff have received adequate and regular training.~~The Supplier Code of Conduct must be signed by suppliers, and confirms that bribery and corruption is not tolerated. Detective Controls: Pass rate and number of test attempts is monitored to identify risk areas and any additional training or guidance required.	The People Function~~Human Resources~~ is responsible for any incidents where further action is required and ensuring completion of mandatory training Procurement Financial Crime Team is responsible for reviewing training effectiveness.	Ongoing Ongoing
Conflicts of Interest	The acceptance of hospitality or gifts from third parties could lead to bias or undue influence, or the perception of such, in how individuals exercise their duties and responsibilities.	Preventative Control: The Group operates a procedure to ensure Gifts and Hospitality may not be offered or accepted where they could bias or influence how individuals exercise their duties and responsibilities. All employees are made aware of and are expected to comply	All employees	Ongoing

Commented [SS13]: Changed title

Commented [ML12]: Amended to incorporate supplier code of conduct which serves to mitigate this risk

POL00423570

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
		with the gifts and hospitality procedures.		
Employment Risks	Failure to identify employees requesting or receiving something of value from a third party in exchange for providing employment or work opportunities may result in the loss of Group stakeholder support.	Preventative Control: Any form of employment or work opportunities (paid or unpaid) must be reviewed and approved in accordance with HR policies and procedures prior to employment.	Line Managers and ~~HR~~ People Business Partner	Ongoing
Existing Employees	Where there are work opportunities with high reward packages, or a significant element of judgment in awarding elements of the package, for instance bonuses, expenses, compensation or sales incentives, an employee may feel it's worth bribing the decision maker.	A formal performance development plan is in place for all employees, ensuring performance is documented against Post Office values & behaviours, with formal objectives aligned to business strategy. A Remuneration Policy exists and is updated annually	~~HR~~The People Function ~~HR~~The People Function	Ongoing Ongoing
Gifts	Inadequate controls may lead to employees offering or accepting gifts that are not appropriate, proportionate or within policy resulting in reputational damage or criminal prosecution.	Preventative Control: All employees must report correctly, and receive approval for, all gifts of £20 and over which they receive or offer using the Gifts & Hospitality tool, whether accepted or declined.	Each employee is responsible for ensuring that all gifts offered or received is~~are~~ recorded. Line managers are responsible for ensuring	Ongoing Ongoing

Commented [SS14]: Changed title

Commented [SS16]: Changed title

Commented [SS17]: Changed title

Commented [ML15]: Risk and Minimum Control Standards included to cover internal bribery risks, and a recommendation is made in the ABC risk assessment that this policy is updated.

Commented [ML18]: To cover that approval must be given prior to accepting/offering.

POL00423570

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
		~~No employee may~~The acceptance ~~accept~~ of cash (or cash equivalent) gifts is prohibited.	the gift complies with policy and is reasonable, and for approving or declining the acceptance of a gift.	
		Post Office has a Group wide training programme to ensure that all customer facing staff, back office staff and contractors receive adequate training. Staff and contractors are required to complete training within 30 days of joining Post Office and annually.	Group Executive are responsible for approving or declining any offers or receipts over £100.	Ongoing
			Financial Crime Team is responsible for reviewing and monitoring the Gifts and Hospitality register.	Ongoing
		Corrective Control: Where discrepancies of non-conformance with gifts and hospitality reporting are identified, line management should consider action under the Conduct Code	~~Human Resources~~The People Function is responsible for any incidents where further action is required and ensuring completion of mandatory training	Ongoing
		Any gift received which is not approved by Line Manager/GE or which is outside policy must be returned.	Line Manager	Ongoing

Commented [SS19]: Control re-inforced

Commented [SS21]: Changed title

Commented [SS20]: Added to reinforce control

POL00423570

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
Hospitality	Inadequate controls may lead to employees offering or accepting hospitality that is not appropriate, proportionate or within policy resulting in reputational damage or criminal prosecution.	Preventative Control: All employees must report correctly, and receive approval for, any hospitality which they receive or offer using the Gifts & Hospitality tool, whether accepted or declined.	Each employee is responsible for ensuring that all hospitality offered/received is recorded	Ongoing
		Before accepting or giving hospitality an employee must receive written approval from their line manager.	Line managers are responsible for ensuring the hospitality complies with policy and is reasonable and for approving or declining the acceptance of hospitality	Ongoing
		The hospitality must be reasonable (not lavish or extravagant), proportionate to its purpose and must ordinarily be below £200 per person in value.	Group Executive are responsible for the approving or declining of any offers or receipts of hospitality over £200.	Ongoing
		Post Office has a Group wide training programme to ensure that all customer facing staff, back office staff and contractors receive adequate training. Staff and contractors are required to complete training within 30 days of joining Post Office and annually.	Financial Crime Team is responsible for reviewing and monitoring the Gifts and Hospitality register	Ongoing
		Corrective Control: Where discrepancies of non-conformance with gifts and	~~Human Resources~~The People Function is	Ongoing

Commented [ML22]: To cover that approval must be given prior to accepting/offering.

Commented [SS23]: Changed title

POL00423570

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
		hospitality reporting are identified, line management should consider action under the Conduct Code.	responsible for any incidents where further action is required and ensuring completion of mandatory training	
Payment Risks	Offering facilitation payments, gifts & entertainment, client training programmes, charitable or political donations, ex-gratia payments or legal settlements that are not justifiable or proportionate may result in reputational damage or criminal prosecution.	Preventative Control: All employees are required to comply with the conflicts of interest policy which can be found here. All employees are required to comply with the Gifts and Hospitality procedure which can be found here. The acceptance of discounted or complimentary training courses which would usually incur a cost are classified as Gifts and Hospitality and employees are required to report these using the Gifts & Hospitality Tool. The payment of ex-gratia payments or legal settlements are strictly controlled and must be submitted to the Group Legal Director for approval.	Each employee is responsible for ensuring that all hospitality and gifts offered or received are recorded. Line managers are responsible for approving or declining the acceptance of a gift or hospitality. Group Executive are responsible for the approving or declining of any offers of gifts or hospitality over the agreed amounts Financial Crime Team is responsible for reviewing and monitoring the Gifts and Hospitality register	Ongoing Ongoing Ongoing Ongoing

POL00423570

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
		Any gift received which is not approved by Line Manager/GE or which is outside policy must be returned.	Line Manager	Ongoing
		Post Office has a Group wide training programme to ensure that all customer facing staff, back office staff and contractors receive adequate training. Staff and contractors are required to complete training within 30 days of joining Post Office and annually.	Group Legal Director is responsible for reviewing and signing off as required any ex-gratia payments or legal settlements as requested from the Business. ~~Human Resources~~The People Function is responsible for any incidents where further action is required and ensuring completion of mandatory training	Ongoing
Political Donations/Lobbying	Employees making or soliciting political donations on behalf of Post Office may result in criminal prosecution.	Preventative Control: Before giving or offering Hospitality to or from a political party, approval must be obtained from a GE Member. The giving of political donations or gifts on behalf of the group to a Politician or a Political Party is strictly prohibited.	Each employee is responsible for ensuring that all Gifts & Hospitality offered or received is recorded Group Executive are responsible for the approving or declining of any offers of hospitality by a political party	Ongoing Ongoing

Commented [SS24]: Changed title

POL00423570

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

Commented [SS25]: Changed title

Commented [ML26]: Included as per ABC risk assessment recommendations

POL00423570

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

POL00423570

3. Definitions

3.1. Definitions

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

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

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

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

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

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

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

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

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

POL00423570

4. Where to go for help

4.1. Additional Policies

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

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

4.2. How to raise a concern

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

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

- their line manager,
- a senior member of the HR Team, or
- if either or both are not available, staff can contact the Post Office's General Counsel, who can be contacted by email at: whistleblowing GRO or by telephone on GRO
- the confidential Whistleblowing Speak Up service 'Ethicspoint' provided by Navex Global via telephone on GRO
- or via a secure on-line web portal: http://postoffice.ethicspoint.com/https://secure.ethicspoint.eu/domain/en/report_custom.asp?clientid=106826

Commented [VC27]: Updated web address

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

4.3. Who to contact for more information

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

11

POL00423570

5. Governance

5.1. Governance Responsibilities

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

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

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

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

POL00423570

6. Control

6.1. Policy Version

Date	Version	Updated by	Change Details
November 2016	1	Georgina Blair	Roll out of Final version
June 2017	1.2	Thomas Richmond	Updated in line with comments from stakeholders
July 2017	1.3	Sally Smith	POL R&CC approval
September 2017	2	Sally Smith	Final Version approved by ARC
June 2018	2.1	Sally Smith	Annual revisions
July 2018	2.2	Sally Smith	POL R&CC approval
July 2018	2.3	Sally Smith	POL ARC approval
September 2018	2.4	Sally Smith	POMS ARC approval
September 2018	3	Thomas Richmond	Final Version approved by ARC's
July 2019	3.1	Sally Smith	Annual review
July 2019	3.2	Sally Smith	POL R&CC approval
September 2019	3.3	Sally Smith	POMS ARC approval
September 2019	4.0	Sally Smith	Final version approved by ARC's
April 2020	4.1	Sally Smith	Updated with new Speak Up service contact details
June 2020	4.2	Sally Smith	Annual revisions

6.2. Policy Approval

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

Committee	Date v. 4.0 Approved
POL R&CC	4th July 2019
POL ARC	29th July 2019
POMS ARC	19th September 2019
Committee	**Date approved**
POL R&CC	
POL ARC	
POMS ARC	

Policy Sponsor: Group Director of Legal, Compliance~~Risk~~ & Governance

Policy Owner: Director of Compliance

Policy Author: Head of Financial Crime

Next review: July 2021~~2019~~

11

Company Details

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

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

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

POL00423570

Appendix A

GIFTS AND HOSPITALITY POLICY

All gifts and hospitality received and offered by Post Office employees must be reported on the central register and **pre-approved prior to acceptance***. This to ensure that Post Office is transparent in its dealings with third parties and suppliers and to enable senior management and the GE to monitor the level of gifts and hospitality both received and offered across the business.

All employees receive annual training as part of the Anti-Bribery & Corruption module within 30 days of joining Post Office and annually.

Gifts:

- All employees are responsible for ensuring that full details of gifts are accurately recorded including the recipients details and a description of the gift, dates of offer and the amount – if a gift is received by a Post Office employee, then an approximate value can be recorded, if known, or the offeror must be contacted and asked the amount so that this can be properly recorded.
- All gifts of £20 and over which are received or offered must be recorded using the Gifts & Hospitality tool, whether accepted or declined by the receiver.
- Line managers must review and approve all gifts over £20. If a gift is over £100, then this must also be reviewed and approved by the GE member for that area
- Before any gift is offered by a Post Office employee, they must refer to the relevant cost centre budget holder for approval before proceeding
- No employee may accept cash (or cash equivalent) gifts (including gift cards).
- The value of the gift must be appropriate and proportionate for the roles and relationship with the client
- Any offer must have a clear and demonstrable link with a legitimate business purpose, gifts must never be accepted from a third party who is tendering for business with Post Office.
- Recipients or offerors must consider if an offer could be viewed by an external party as inappropriate. Guidance can be sought from line management or by raising a query via gifts.hospitality GRO

Hospitality:

- All employees are responsible for ensuring that full details of hospitality are recorded including the recipients details and a description of the hospitality, details of venue/event, dates of offer and event and the amount – if the amount is not known the offeror must be contacted and asked the amount so that this can be properly recorded
- All hospitality which is received or offered must be recorded using the Gifts & Hospitality tool, whether accepted or declined by the receiver.
- Line managers must review and approve all hospitality. If hospitality is over £200, then this must also be reviewed and approved by the GE member for that area
- Before any hospitality is offered by a Post Office employee, they must refer to the relevant cost centre budget holder for approval before proceeding
- The value of the hospitality must be appropriate and proportionate for the roles and relationship with the client
- Any offer must have a clear and demonstrable link with a legitimate business purpose, hospitality must never be accepted from a third party who is tendering for business with Post Office.
- Recipients or offerors must consider if an offer could be viewed by an external party as inappropriate. Guidance can be sought from line management or by raising a query via gifts.hospitality GRO

POL00423570

- Small offers of hospitality such as tea, coffee, sandwiches, etc. do not need to be recorded via the gifts and hospitality tool, but the recipients details must be recorded fully on the expenses claim via Selenity Expense reporting tool

* Where it is not possible to record gifts and hospitality received prior to receipt, for example where a gift is received unexpectedly, or where a client offers to pay for lunch, then this must be recorded **on the next available day** and the reasons for late approval should be added in the comments box. For offers of hospitality verbal approval from a more senior manager should be obtained.

POL00423570

POST OFFICE LIMITED RISK & COMPLIANCE COMMITTEE REPORT

Title:	**Annual Whistleblowing Report**	**Meeting Date:**	13th July 2020
Author:	**Sally Smith**	**Sponsor:**	Ben Foat

Input Sought: Discussion

The committee is asked to review the contents of this report, approve the updated Whistleblowing Policy and consider whether any further actions should be taken to improve Whistleblowing reporting and management.

Previous Governance Oversight

The last annual Whistleblowing report and Policy amends were approved in July 2019

Executive Summary

The whistleblowing process within Post Office is robust and the volume of whistleblowing reports is consistent year on year. Monthly MI is produced to track and monitor reports and investigations.

Further work is recommended to raise staff awareness and a continuous awareness and improvement programme is being delivered by the Financial Crime team.

Policy changes are minor and require no additional actions.

POL00423570

Questions addressed

1. What issues have been highlighted by the annual review of Whistleblowing reports?
2. What actions need to be undertaken to address any issues?
3. What changes to the Policy do we propose and why?
4. What are the implications of these changes?

Report

Summary of activities relating to Whistleblowing reporting 2019/20:

5. The Financial Crime team co-ordinate all whistleblowing reports and investigation on behalf of the Whistleblowing Officer, ensuring all significant or sensitive allegations are referred to the Whistleblowing Officer and that a monthly report on cases and activity is provided. A process document was created to provide guidance on how to deal with Whistleblowing reports received via all channels, including guidance for investigating managers.
6. The Financial Crime Policy Assurance Framework review which assesses if minimum control standards in policies are being met across the group was developed further during the year and the quarterly reviews have identified no deficiencies or major flaws in the application of the Whistleblowing Policy across Post Office (please refer to Appendix B for latest assurance status).
7. Our external whistleblowing reporting channels supplier, Expolink Europe Ltd, was acquired by Navex Global in June 2019. A new contract with Navex Global to provide Whistleblowing services has been completed and Post Office migrated onto their new reporting platform.
8. In 2019/20 there were 6 communications published relating to Whistleblowing to raise awareness of the reporting channels and protections, and encourage reports to be made, and some workshop sessions were held at the Employee Engagement Conference to explore ethical values and 'doing the right thing'.

Annual Policy review:

9. There have been no regulatory or legislation changes.
10. Following annual review, only minor amends have been made to clarify wording and definitions within the overview and minimum control standards sections.

Summary of Whistleblowing reports received 2019-20

11. Year on year comparison shows that there has been a slight decrease in whistleblowing reports from 43 in 2018/19 to 41 in 2019/20 (please refer to Appendix A for further details).
12. Most reports relate to individuals in the network – Postmasters and Agent Assistants as well as Post Office employees. Although there has been an increase in reports relating to colleagues in our supply chain cash centres.
13. The most popular reporting channel continues to be the Speak Up line. There has been a 59% decrease in anonymous reports being submitted, indicating that reporters have increased trust in Post Office to manage their concerns effectively.
14. The most common complaint relates to fraud, and 5 out of the 7 allegations are against Postmasters. There was also an increase in reports with allegations of Money Laundering & Bribery and Corruption.

POL00423570

15. There have been several reports relating to one non-customer facing location. HR continue to investigate if there are any underlying root causes or issues at this location.

16. There have been some delays in investigation caused by the Covid lockdown and inability of investigating managers to travel, but these can now be fully investigated.

Risk Assessment, Mitigations & Legal Implications

17. The new contract and the migration to the new Whistleblowing service with Navex was completed without any major problems or risks being identified. This also removed a previously identified contractual risk, for which there had been an approved risk exception note.

18. During 2019/20 there were no regulatory or legislative changes to Whistleblowing requirements, and no matters raised of material concern.

Stakeholder Implications

19. The Whistleblowing Policy makes reference to Post Office Investigations policy, specifically in relation to internal matters, however, this policy is currently out of date. The People and Policy Compliance Manager has scheduled work to get this updated for the September 2020 RCC.

Next Steps & Timelines

20. A Whistleblowing communications plan has been developed for the current year with a focus on increasing awareness around the new service and the new reporting channels.

21. Additionally a training awareness presentation or animation is planned for the second half of 2020/21.

POL00423570

GROUP POLICIES

Whistleblowing Policy

Version – V4.2

11

Chief Executive's Endorsement

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

POL00423570

1. Overview 3
1.1. Introduction by the Policy Owner 3
1.2. Purpose 3
1.3. Core Principles 3
1.4. Application 43
1.5. Legislation 4
1.6. What is Whistleblowing 4
1.7. Protecting the whistleblower ..... Error! Bookmark not defined.4
1.8. Whistleblowing Officer and 'Speak Up' ..... Error! Bookmark not defined.5
1.9. External Disclosures 65
2. Risk Appetite and Minimum Control Standards 87
2.1. Risk Appetite 87
2.2. Policy Framework 87
2.3. Who Must Comply? 87
2.4. Minimum Control Standards 98
3. Definitions 1413
3.1. Definitions 1413
4. Where to go for help 1514
4.1. Additional Policies 1514
4.2. How to raise a concern 1514
4.3. Who to contact for more information 1514
5. Governance 1615
5.1. Governance Responsibilities 1615
6. Control 1716
6.1. Policy Version 1716
6.2. Policy Approval 1716
Company Details 1716

11

POL00423570

1. Overview

1.1. Introduction by the Policy Owner

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

1.2. Purpose

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

Commented [SS1]: Words added in footnote to add further clarification re group

Commented [EF2]: Footer definition expanded to include 'employees' and 'staff'

1.3. Core Principles

"Whistleblowing" refers to the act of exposing potential or actual wrongdoing, misconduct and/or dangerous practices by reporting it either internally within an organisation, or to an external party. A whistleblower is a person who raises a genuine concern in relation to any wrongdoing, this includes criminal activity, regulatory breaches, miscarriages of justice, damage to the environment, financial impropriety, reputational damage, any breach of legal or professional obligations, dangers to health and safety and the deliberate attempt to conceal it. In order to encourage Whistleblowing and provide appropriate protections to whistleblowers, the governance arrangements described in this Policy are based upon the following core principles:

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

11

[1] In this Policy "Post Office" and "Group" mean Post Office Limited and any wholly owned subsidiary that formally adopts this policy.

[2]. In this Policy "employee" and "staff" means POL or Group's permanent, temporary and fixed term employees, workers including temporary workers, agency workers (where the terms on which they are engaged are not substantially determined by them), contractors, consultants and anyone else working under a contract with Post Office, in all cases having regard to s.230(3) and s. 43K Employment Rights Act 1996.

POL00423570

1.4. Application

This Policy is applicable to all staff within the Group and outlines the manner in which Post Office will encourage, receive and investigate incidents of whistleblowing and the protections provided for whistleblowers by law.

In order to encourage reporting of wrongdoing, Post Office will, where appropriate, and to the extent possible, follow equivalent principles to encourage, receive and investigate incidents of whistleblowing by Postmasters, Agent Assistants, and members of the public and will not subject any such persons to any detriment (including the termination of any contract or relationship with Post Office) for raising a genuine whistleblowing concern in an appropriate manner.

1.5. Legislation

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

- Employment Rights Act 1996
- Public Interest Disclosure Act 1998

1.6. Protecting the Whistleblower (Your Legal Rights)

Post Office has a statutory obligation to protect whistleblowers and will support any individual person who raises genuine concerns under this Policy in an appropriate manner, even if they turn out to be mistaken. In respect of a certain class of person (broadly "staff" as defined under this policy) Post Office has a statutory obligation not to subject such persons to detriment or to dismiss them for whistleblowing.

Where a member of staff is subject to a Post Office settlement agreement, any clauses within it will not prevent the member of staff from whistleblowing. This should in any event be made clear by the terms of the settlement agreement itself and staff should receive independent advice in relation to those terms when entering into a settlement agreement.

Post Office will, at all times, respect the confidentiality and protect the whistleblower's identity, however:

- It may be necessary in the course of an investigation to share this information with a relevant stakeholder (e.g. an investigator).
- There is no requirement for a whistleblower to provide personal contact information, but not providing this information may reduce Post Office's ability to undertake a thorough investigation into the concerns raised.

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

If a whistleblower believes that they have suffered any such treatment, they should inform the Whistleblowing Officer immediately. The Whistleblowing Officer or nominated ~~representative~~deputy will~~should~~ take all necessary steps at the earliest opportunity to address any victimisation, which may include working with the HR team to put

Commented [EF3]: Reworded for clarity

11

POL00423570

appropriate remedial measures in place. If the matter is not addressed the whistleblower (where they are staff) should raise it formally using Post Office's Grievance procedure.

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

1.7 The Whistleblowing Officer

Post Office has appointed the General Counsel as the Whistleblowing Officer who can be contacted at whistleblowing GRO or by telephone on: GRO

The role of the Whistleblowing Officer and their nominated deputies is to receive all internal reports raised, regardless of the channel used, review any concerns raised and determine the best course of action, if any. They may ask for further information in order to make this decision.

Commented [EF4]: Clarity re. nominated deputies appointed by the Whistleblowing Officer

The Whistleblowing Officer is also responsible for ~~the~~ Post Office's overall Whistleblin~~gewer P~~policy and governance framework, which ~~ensuresing~~ that reports are investigated and responded to in a timely manner. They are responsible for determining the appropriate parties who should investigate the allegations raised, taking into account the sensitivities and seriousness of the report and the need to protect the whistleblower.

Commented [EF5]: Reworded for clarity

The Whistleblowing Officer is also responsible for identifying key trends or issues, and providing assurance to the Board that the policy is complied with.

1.8 How to Report Whistleblowing

Post Office supports and promotes a number of reporting mechanisms:

- Direct to the Whistleblowing Officer (whistleblowing GRO
- Via a complaint to a front line team, e.g. customer complaints, BSC and Grapevine. These may be verbal or written communications.
- Contacting the "Speak Up" line, a confidential reporting service which is run by an independent company NAVEX Global (formerly Expolink Europe Ltd)

~~Contact details for~~ the Speak Up line are:

- GRO
- http://postoffice.ethicspoint.com/~~https://secure.ethicspoint.eu/domain/en/report_custom.asp?clientid=106826~~ which is a secure on-line web portal

Commented [EF6]: Updated web address

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

- Where Post Office or the Group is in breach of any legal obligation to which it is subject (usually a statutory rather than a contractual legal obligation)
- Financial Crime including Fraud, Money Laundering and financing of terrorism,
- Giving, offering or taking of bribes originating both inside or outside Post Office but related to Post Office business activities,
- Financial mismanagement, Tax evasion and Misreporting
- Racial, sexual, disability or other discrimination (Improper Behaviour),
- Practices that could put individuals or the environment at risk,
- Breach of Post Office internal policies and procedures
- Concerns about slavery or human trafficking[3], and
- Any conduct likely to damage Post Office's reputation

Commented [EF7]: Wording added for clarity

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

POL00423570

This policy should not be used by staff wishing to raise complaints relating to their own personal circumstances, such as the way they have been treated at work. Grievances and matters such as bullying and harassment should be raised in accordance with the procedures set out in the appropriate HR policy.

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

1.9 Responding to Whistleblowing Reports

In all instances any whistleblowing reports, regardless of reporting method, will be responded to within 5 working days and passed onto the Whistleblowing Officer.

All reports will be fully reviewed and investigated and any information, including emails, or records of telephone calls, letters, or any other form of communication stored securely and confidentially.

The time frame for investigating the reports raised is dependent on the nature of the report and the investigation required, however, the whistleblower will be given feedback via the reporting channel they have used, or have given the Whistleblowing Officer permission to use (Speak Up line, e-mail or phone call) during the investigation and once it has been concluded.

The whistleblower may be kept informed of any action taken, however, this information may be limited if it is required to keep the confidence of other people.

Where a report received is anonymous, whistleblowers will not ordinarily be able to receive feedback and details of action taken by Post Office may be limited.

1.10 External Disclosures

The aim of this Policy is to provide an internal mechanism for reporting, investigating and remedying any wrongdoing in the workplace and to demonstrate Post Office's commitment to listen to the concerns of workersstaff. In most cases individuals should not find it necessary to alert anyone externally.

Commented [SS8]: Wording added to reinforce culture

However, the law recognises that in some circumstances it may be appropriate for individuals to report their concerns to an external body such as a regulator. It will rarely, if ever, be appropriate to alert the media at least without informing Post Office or an external agency first and usually in that order.

We strongly encourage individuals to seek advice before reporting a concern to anyone external. The independent whistleblowing charity, Protect (formerly Public Concern at Work) have a list of prescribed regulators for reporting certain types of concerns. Their contact details are as follows:

Helpline: GRO
Website: www.pcaw.org.uk/advice-line/

Protect operates free, confidential advice to people concerned about crime, danger or wrongdoing in the workplace. All Protect advisors are legally trained and supervised by qualified lawyers and their advice is fully confidential and subject to legal privilege. All

POL00423570

information, including emails, or records of telephone calls, letters, or any other form of communication with Protect advisors is stored in a fully encrypted format.

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

Helpline: GRO
E-mail: whistle@fca.org.uk
Website: www.fca.org.uk/site-info/contact/whistleblowing
Address: Intelligence Department (Ref PIDA), Financial Conduct Authority, 12 Endeavour Square, London, E20 1JN
Whistleblowing concerns usually relate to the conduct of our staff, but they may sometimes relate to the actions of a third party, such as a customer, supplier, agent, Postmaster or service provider. In some circumstances the law will protect individuals if they raise the matter with the third party directly. However, we encourage individuals to report such concerns internally in the first instance.

POL00423570

2. Risk Appetite and Minimum Control Standards

2.1. Risk Appetite

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

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

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

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

2.2. Policy Framework

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

2.3. Who Must Comply?

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

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

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

POL00423570

2.4. Minimum Control Standards

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

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

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
Receipt and investigation of whistleblowing reports	Failure to meet legal and regulatory requirements	Directive Control: Post Office must nominate a Whistleblowing Officer to receive reports, ensure that all reports are fully investigated and that any appropriate corrective action is undertaken.	Post Office CEO and Board	Ongoing
		The Whistleblowing Officer must provide a whistleblowing report to the R&CC and ARC at least annually.	Whistleblowing Officer	Annually
		Any serious whistleblowing concerns must be promptly escalated to the Chairman of the Post Office Audit and Risk Committee.	Whistleblowing Officer	Ongoing
		Preventative Control: All employees are trained and the policy is available to them	Whistleblowing Officer	Training must be provided at least annually and within 30

POL00423570

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
		The Whistleblowing Officer must ensure that appropriate arrangements are in place to ensure that whistleblowing reports are addressed promptly including during absences.	Whistleblowing Officer	days of joining Post Office Ongoing
		Communications and awareness provided to all employees ~~and Policy document published on the Intranet~~.	Head of Financial Crime	Ongoing~~Annuall y~~
		Corrective Control The Whistleblowing Officer must escalate WB reports to the appropriate Investigating manager for investigation to take place.	Whistleblowing officer	Ongoing
		The nominated Investigating manager responsible for conducting the investigation must report the findings back to the Whistleblowing Officer	Investigating manager	Ongoing
Breach of confidentiality	Failure to ensure confidentiality for the whistleblower	Preventative Control: Whistleblowing Policy is robust and up to date.	Whistleblowing Officer	Ongoing
		Confidential Speak Up line reports are shared only with the Whistleblowing Officer and nominated deputies	Whistleblowing Officer	Ongoing
		Whistleblowing email inbox access is restricted to the	Whistleblowing Officer	Ongoing

Commented [EF11]: Clarity of training requirement

Commented [EF9]: Correction of wording

Commented [EF10]: 2 new minimum control standards added to reflect practice

Commented [EF12]: Reworded for clarity

POL00423570

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
		Whistleblowing Officer and nominated deputies		
		Whistleblowing Officer must put arrangement in place to protect the confidentiality of the whistleblower during investigations	Whistleblowing Officer	Ongoing
		Corrective Control: All incidents of breaches are escalated to the Whistleblowing Officer to review and take necessary actions.	Whistleblowing Officer	Ongoing
Incorrect handling of whistleblowing report	An individual may raise a whistleblowing report with other individuals in the Group. Details may then be shared with various stakeholders before being passed onto the Whistleblowing Officer	Preventative Control: Training provided to contact teams to identify potential whistleblowing reports and ensure these are correctly handled, e.g.: • Grapevine, • NBSC, • Customer Support, and • Executive Correspondence Team.	Whistleblowing Officer	Annually and within 30 days of joining the Post Office
		Communications and awareness provided to all employees. and ~~Policy document published on the Intranet.~~	Head of Financial Crime	~~Annually~~ Ongoing
		Corrective Control: All incidents of breaches are escalated to the Whistleblowing	Whistleblowing Officer	

Commented [EF14]: Clarity of training requirement

Commented [EF13]: Correction of wording

POL00423570

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
		Officer to investigate and take appropriate actions.		Ongoing
Insufficient Information	Failure to capture/report sufficient information about the issue may mean that the underlying issue cannot be properly investigated and resolved	Directive Control: Individuals are encouraged to report issues and provide full information and their contact details, where they feel able to do so. Corrective Control: All reports, including those where insufficient information has been provided and no further action was taken are recorded on the Whistleblowing database, which is reviewed for trends and issues.	Whistleblowing Officer Whistleblowing Officer	Ongoing Ongoing
The 'Speak Up' Service	Failure to effectively record whistleblowing reports and pass onto the Whistleblowing Officer, due to factors such as resource or IT failure.	Preventative Control: The Whistleblowing Officer must review the effectiveness of the service provided by NAVEX Global (formerly known as Expolink Europe Ltd) at least annually. The Whistleblowing Officer must review the effectiveness of the processes operated by Grapevine, BSC, Customer Support, and The Executive Complaints Team at least annually to ensure that whistleblowing reports are	Whistleblowing Officer Whistleblowing Officer	Annually Annually

POL00423570

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
		identified and communicated promptly.		
Treatment of Whistleblowers	Breach of whistleblowing guidelines such that a whistleblower suffers prejudice, detriment or dismissal as a result of making a whistle blowing report	Preventative Control Training must be provided to all people managers as part of their induction process as a manager and on appointment to Post Office	Whistleblowing Officer and ~~HR~~ People Training Manager	Ongoing
		Annual training must be provided to all Post Office staff to remind them of the protections available to whistleblowers and the importance of identifying and reporting wrongdoing	Whistleblowing Officer and ~~HR~~ People Training Manager	Ongoing
		The Code of Business Standards must refer to the whistleblowing policy and must be provided to all new joiners as part of their induction programme.	Whistleblowing Officer and ~~HR~~ People Training Manager	Ongoing

Commented [SS15]: Changed title

POL00423570

3. Definitions

3.1. Definitions

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

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

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

Commented [EF16]: Correction of team name

Telephone Number: GRO
E-mail: nbscenquiries GRO

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

E-mail: customercare GRO

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

E-mail: flagcaseadviso GRO

POL00423570

4. Where to go for help

4.1. Additional Policies

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

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

4.2. How to raise a concern

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

- Their line manager,
- A senior member of the HR Team, or
- If either or both are not available, staff can contact the Post Office's Whistleblowing Officer, who can be contacted by email at: whistleblowing GRO or by telephone on: GRO
- the confidential Whistleblowing Speak Up service 'Ethicspoint' provided by Navex Global via telephone on: GRO
- or via a secure on-line web portal: http://postoffice.ethicspoint.com/~~https://secure.ethicspoint.eu/domain/en/report_custom.asp?clientid=106826~~

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

Commented [EF17]: Updated web address

4.3. Who to contact for more information

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

11

POL00423570

5. Governance

5.1. Governance Responsibilities

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

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

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

POL00423570

6. Control

6.1. Policy Version

Date	Version	Updated by	Change Details
April 2016	1.4	Jane MacLeod	Sponsors review and sing-off
August 2017	1.5	Vitor Camara	Annual Review and update.
September 2017	1.6	Thomas Richmond	POL R&CC approval
September 2017	2	Thomas Richmond	Final version approved
June 2018	2.1	Vitor Camara	Annual review and update.
July 2018	2.2	Sally Smith	POL R&CC approval
July 2018	2.3	Sally Smith	POL ARC approval
September 2018	2.4	Sally Smith	POMS ARC approval
September 2018	3	Vitor Camara	Final version approved
June 2019	3.1	Sally Smith	Annual review and update
June 2019	3.2	Sally Smith	Incorporating legal review comments
July 2019	3.3	Sally Smith	POL R&CC approval
September 2019	3.4	Sally Smith	POMS ARC approval
September 2019	4.0	Sally Smith	Final version approved
April 2020	4.1	Sally Smith	Updated with new Speak Up service contact details
June 2020	4.2	Sally Smith	Annual review and update

6.2. Policy Approval

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

Committee	Date 4.0 Approved
POL R&CC	4th July 2019
POL ARC	29th July 2019
POMS ARC	19th September 2019
Committee	Date Approved
POL R&CC	
POL ARC	
POMS ARC	

Policy Sponsor: Group Director of Legal, Compliance & Governance
Policy Owner: Whistleblowing Officer
Policy Author: Head of Financial Crime

Next review: July 2021~~0~~

Company Details

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

POL00423570

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

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

POL00423570

GROUP POLICIES

Financial Crime Policy

Version – V4.2

11

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

POL00423570



1. Overview 3
1.1. Introduction by the Policy Owner 3
1.2. Purpose 3
1.3. Core Principles 3
1.4. Application 3
1.5. Financial Crime Risk 4
1.6. Legislation 5
2. Risk Appetite and Minimum Control Standards 6
2.1. Risk Appetite 6
2.2. Policy Framework 6
2.3. Who must comply? 7
2.4. Minimum Control Standards 8
2.5. Product and Service Risk Tools 1513
3. Where to go for help 1714
3.1. Additional Policies 1714
3.2. How to raise a concern 1714
3.3. Who to contact for more information 1714
4. Governance 1815
4.1. Governance Responsibilities 1815
5. Control 1916
5.1. Policy Version 1916
5.2. Policy Approval 1916
Company Details 1916

11

POL00423570

1. Overview

1.1. Introduction by the Policy Owner

The General Counsel has overall accountability to the Board of Directors for the design and implementation of controls to prevent or deter Financial Crime. Financial Crime is an agenda item for the Audit and Risk committees and the Post Office board is updated as required.

1.2. Purpose

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

Commented [SS1]: Definition updated to include 'employee' and 'staff'

1.3. Core Principles

The governance arrangements described in this Policy are based upon the following core principles:

- The interests of stakeholders are protected by ensuring that excessive powers are not delegated to individuals;
- Decisions taken by management are consistent with the Group's strategic objectives and Risk Appetite, which are approved by the Board;
- Appropriate conduct is demonstrated in executing the requirements contained within the Policy;
- Every member of staff is responsible for understanding and managing the risk they take on behalf of the Group;
- Clear accountabilities are delegated by management to people who have the right level of skill, competency and experience;
- All staff are required to comply with Group Policies.

1.4. Application

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

11

[1] In this Policy "Post Office" and "Group" mean Post Office Limited and any wholly owned subsidiary that formally adopts this policy ~~In this policy "Post Office" and "Group" mean Post Office Limited and wholly owned subsidiary.~~

[2] In this policy "employee" and "staff" means all persons working for the Group or on our behalf in any capacity including employees at all levels, directors, officers, agency workers, seconded workers, volunteers, interns, and contractors. ~~In this policy "staff" means permanent staff, temporary including agency staff, contractors, cconsultants and anyone else working for or on behalf of Post Office.~~

POL00423570

In exceptional circumstances, where risk sits outside of the Group's accepted Risk Appetite a Risk Exception can be granted.
Further information in relation to the risk exception process, together with a template can be found here.

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

Failure to comply with the requirements of this policy by any member of staff[2] will be regarded as a significant breach impacting on the Group's risk and control environment and may lead to disciplinary action up to and including dismissal and possible prosecution.

The risk to the Group in relation to Financial Crime is reviewed by the board on a regular basis.

1.5. Financial Crime Risk

"Financial Crime" is any offence involving: fraud or dishonesty, misconduct in, or misuse of information or handling the proceeds of crime. It can be internal (by individuals within an organisation) or external (by criminals using an organisation to facilitate financial crime). Financial Crime is commonly considered as including one or a combination of the following offences:

- fraud
- ~~electronic~~ Cybercrime
- money laundering
- terrorist financing
- bribery and corruption
- information security

Commented [ML2]: More well-known term and links to reference made in External Financial Crime section

Failure to manage Financial Crime risks and incidents appropriately could result in financial loss, customer impact, regulatory breaches, fines, prosecution, prevention from selling a particular product, loss of existing or future contracts/relationships and damage to reputation.

These risks include, but are not limited to, the following:

External Financial Crime:
The risk of external events due to acts of a type intended to defraud, steal or misappropriate assets/ property, or which seek to circumvent the law, by a third party. Examples would include:

- Any dishonest or fraudulent act,
- Theft of assets from an organisation or its customers,
- Card or account abuse or account takeover by a third party,
- Counterfeit payment instruments (cards, cheques, etc.) and identity documents,
- ATM fraud and theft,
- Online or mobile fraud,
- Cyber Crime, and

POL00423570

- Social engineering fraud.

Internal Financial Crime
The risk of internal events due to acts of a type intended to defraud, steal or misappropriate assets/property, or which seek to circumvent regulations or the law applicable to an organisation or its contracts or internal policies or procedures. Examples would include:

- Any dishonest or fraudulent act circumventing regulations or law,
- Profiteering as a result of insider knowledge of an organisation's activities,
- Theft of assets from an organisation or its customers,
- Manipulation of transactional data at point of sale,
- False expense or payroll claims,
- Manipulation of accounts or financial statements, and
- Breach of internal processes or controls for personal gain.

The Group takes the above internal risks and Financial Crime seriously and will take appropriate action against any person including disciplinary, dismissal and possible prosecution of anyone involved in such events.

1.6. Legislation

There are a number of relevant UK legal and regulatory requirements which describe financial crime including (but not limited to):

- The Fraud Act 2006
- The Bribery Act 2010
- The Theft Act 1968
- Common Law Offences of Fraud in Scotland
- The Proceeds of Crime Act 2002
- The Criminal Finances Act 2017
- Policing and Crime Act 2017
- The Terrorism Act 2000
- The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (known as Money Laundering Regulations 2017) (Amendment made to regulations in 2019)
- Forgery and Counterfeiting Act 1981
- Identity Documents Act 2010

Commented [ML3]: Included to reflect current regulation

The group has regard for guidance and other assistance offered by regulatory, industry and other specialist bodies, for example UK Finance (which incorporates BBA, UK Payments and Financial Fraud Action UL), Link, etc., publish trends and analysis on current threats and issues.

POL00423570

2. Risk Appetite and Minimum Control Standards

2.1. Risk Appetite

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

The Group takes its legal and regulatory responsibilities seriously and consequently has[3]:

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

The Group also has a zero tolerance policy to criminal tax evasion and the facilitation of tax evasion.

The Group acknowledges however that in certain scenarios even after extensive controls have been implemented a product or transaction may still sit outside the agreed Risk Appetite. In this situation, a risk exception waiver will be required (See section 1.4 for further details).

2.2. Policy Framework

Post Office has established a suite of Financial Crime policies and procedures, on a risk sensitive approach, which are subject to annual review. The policy suite is designed to combat money laundering, terrorist financing, bribery and corruption, fraud and ensure adherence to relevant sanctions regimes. They have been developed to comply with applicable legislation and regulation and cover the following specifically:

- The identification through documented risk assessment of potential or inherent and residual Financial Crime risks and the effectiveness of controls associated with them,
- Completing compliance oversight monitoring to test the Group's controls and confirm effectiveness and adherence to Financial Crime policies,
- On a risk sensitive basis, performing due diligence on our employees, agents and third parties,
- Where the Group has primary or contractual responsibility for the customer relationship ensuring Customer Due Diligence, Enhanced Due Diligence and Sanctions checking are set at any appropriate level commensurate with the risk,
- Establishing and maintaining standards for Management Information on Financial Crime. This includes, but is not limited to, record keeping, customer identity documents, reporting of suspicious activity[4] and details of staff training.

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

[4] For more information in relation to the completion and submission of a Suspicious Activity Report please see the Anti-Money Laundering and Counter Terrorism Policy.

POL00423570

This policy provides an overview of the Financial Crime risk and governance framework and the effective system of internal control for the mitigation of Financial Crime risk required across the Group. The Key Financial Crime policies covering the major risk areas to the Group include:

- Anti-Bribery and Corruption Policy
- Anti-Money Laundering and Counter Terrorist Finance Policy
- HMRC Fit & Proper Policy
- Whistleblowing Policy
- Financial Crime Policy

Associated Policies and Processes include:

- ~~Information Security Policy~~
- Protecting Personal Data Policy
- Cyber & Information Security Policy
- Investigations Policy

Commented [ML4]: Including policies within the Info Sec Policy suite

Each of the above policies should be considered and read in conjunction with any other policy where relevant. These policies are supported by the Risk Exceptions process.

2.3. Who must comply?

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

Commented [ML5]: Amended to standardise wording in line with other policies

All Post Office employees are required to report any knowledge or suspicions (internal or external) in relation to Financial Crime please see 3.2 and a failure to do so may amount to a disciplinary offence.

11

POL00423570

2.4. Minimum Control Standards

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

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

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
Proposed product or service	Products, services or relationships with third parties may rely on systems or processes where prevention or detection of financial crime has not been considered in the design, resulting in financial loss (whether to the Group, its customers or suppliers), reputational damage and/or regulatory sanctions.	Preventative Control: As part of the design of a new product or service: • A Product Information Pack (see 2.5 below) must be completed and be fully up to date. ~~with all the relevant product information.~~ • Product or service risks must be considered and documented using the Financial Crime Engagement Tool (see 2.5 below). Prior to launch, the Product Information Pack (PIP) must be reviewed and approved by the Financial Crime Team. The Financial Crime Team adopts a risk based approach to determine when the full risk assessment should be completed, and the PIP will provide them with key information to make an informed decision. If the product is deemed high risk, the assessment will be completed prior to launch, following which the Financial Crime Team may require the	Product Manager Financial Crime Team Product Manager and Financial Crime Team	During design phase Prior to Launch Prior to launch

Commented [ML6]: Included to reinforce responsibility

POL00423570

		Product Manager to make changes to reduce the risks prior to launch. ~~Prior to launch, the Product Information Pack (PIP) must be reviewed and approved by the Financial Crime Team. The Financial Crime Team adopts a risk based approach to determine when the full risk assessment should be completed, and the PIP will provide them with key information to make an informed decision. If the product is deemed high risk, the assessment will be completed prior to launch~~ The product manager/management team is responsible for ensuring their product complies with legal and regulatory requirements in relation to financial crime.	Product Manager	Ongoing

Commented [ML7]: Included to reflect current process

Commented [ML8]: Included to clarify first line responsibilities

POL00423570

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
Existing products and services	Due to changes in law, regulation, incidents, threats or practices over time, there is a risk that the controls to prevent and detect financial crime are no longer adequate.	Preventative Control: Risk assessments must be undertaken at least annually for high risk products and services, where any changes to the product or service (including supplier changes) are made, where an issue is highlighted, significant risk is identified, an incident occurs, or the regulations change	Product Manager	Annually, or at any time there is a change
		The product manager/management team is responsible for ensuring their product complies with legal and regulatory requirements in relation to financial crime.	Product Manager	~~Any time there is a change~~Ongoing
		Prior to the scheduled risk assessment, the Product Information Pack (PIP) must be reviewed and updated by Product Management and provided to the Financial Crime Team.	Product Manager	Any time there is a change
		Prior to any product or service changes being implemented, the Product Information Pack (PIP) must be reviewed and updated by Product ~~and approved by the Financial Crime Team. The~~Management. The Financial Crime Team adopts a risk based approach to determine when the full risk assessment should be completed, and the PIP will provide them with key information to make an informed decision. If the product is deemed high risk, the assessment will be completed prior to change going live.	Product Manager	When there is a material issue or incident
		Where no initial risk assessment was undertaken, product management complete	Product Manager and Financial Crime Team	Any time there is a change

Commented [SS9]: Included to clarify first line responsibilities

Commented [ML10]: Included to clarify requirements for scheduled risk assessments

Commented [ML11]: To reflect that Product Manager is responsible for updating PIP

POL00423570

		a new or update the existing Product Information pack and provide this to the Financial Crime Team. The Financial Crime Team will then agree a timescale ~~must agree a timescale with the Financial Crime Team~~ to complete an risk assessment. ~~and a Product Information Pack.~~		
		Where the reassessed/assessed risk is considered by the Financial Crime Team to rest outside of the Group's Risk Appetite, or where the strength of the controls is deemed inadequate, as part of the Close Down report produced by the team, recommendations will be provided to the Product Manager to implement or improve controls to mitigate the risks. The Product Manager is responsible for producing an action plan outlining how these risks will be mitigated and subsequently enacting the plan. Where risks cannot be sufficiently mitigated in line with the Group's risk appetite then then the risk exception process must be followed.	Financial Crime Team and Product Manager	Annually or when there is a material issue or incident
		Corrective Control: Product Management must implement escalation procedures for when an incident is identified, so that the Financial Crime Team are made aware, and if the product is outsourced to a third party, the third party is made aware. Product Management are responsible for addressing and overseeing any control failings to mitigate financial crime risks.	Product Manager	As and when an incident is identified

Commented [ML12]: Updated to reflect our current process.

Commented [ML13]: Updated to reflect current process

Commented [ML14]: New control to reinforce first line responsibility

POL00423570

		A risk assessment may be undertaken where an issue is highlighted by monitoring or an incident occurs that is deemed to be systemic. ~~Additionally, risk assessment must be undertaken where an issue is highlighted by monitoring or an incident occurs~~		

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
Human Resources	Due to inadequate screening, there is a risk that the Group employs individuals who do not have the legal right to work in the UK or are unfit to undertake the role.	Preventative Control: To minimise the risk of financial crime by employees, Post Office completes employee screening prior to employment. In addition to this, on a regular basis (proportionate to the role) additional checks will be completed to ensure that there is no risk of internal collusion by any of our employees. For further information please see the employee vetting policy.	Group ~~HR Director~~Chief People Officer	Pre-employment and ongoing where required
Operations	Inadequate training, monitoring and control of internal processes and systems may lead to internal fraud or theft by employees	Directive Control: Post Office has developed a Code of Business Standards and model behaviours that set out the expected standards for all employees and contractors – this is made available to all new and existing staff and reinforced in communications Preventative Control: Access to Post Office systems is via unique user log-ins and annual mandatory compliance training is provided to all staff and contractors.	Group Chief People Officer ~~HR Director~~ Chief Information Officer All Employees	Ongoing Ongoing system design and delivery Pre-employment

Commented [EF15]: Amended to reflect current process

Commented [SS16]: Changed title

Commented [SS17]: Changed title

POL00423570

		Post Office expenses and payroll systems include management checks and controls. Detective Control: Audit trails for system access are maintained and monitored appropriately	~~Human Resources~~The People Function are responsible for any incidents where further action is required and ensuring completion of mandatory training Internal Audit	and ongoing where required Ongoing
Risk Area	**Description of Risk**	**Minimum Control Standards**	**Who is responsible**	**When**
Operations	Inadequate building and systems access controls may lead to financial crime that results in financial loss (whether to the Group, its customers or suppliers), reputational damage and/or regulatory sanctions.	Preventative Controls: Relevant business areas including the property and security teams must assess and assure risks relating to employee and customer access to sites, secured areas, systems and software, recommending and implementing additional controls where appropriate. All business areas are responsible for maintaining documented processes and procedures and deploying adequate monitoring and controls to prevent and detect unauthorised access to sites, secured areas, systems and software to prevent financial crime. Detective Control: Audit trails must be maintained so that building and system access can be monitored.	Head of Property ~~Services~~Equipment and Security All employees	Ongoing Ongoing Ongoing

Commented [SS18]: Changed Title

Commented [SS19]: Changed title

POL00423570

		To ensure that the Group's controls remain effective the Group undertakes internal audits to test and assess their effectiveness.	Chief Information Officer and Physical Security Internal Audit	Ongoing
Financial settlement and reconciliation	Inadequate controls and audit trails relating to financial settlement and reconciliation may result in financial loss (whether to the Group, its customers or suppliers), reputational damage and/or regulatory sanctions.	Preventative Controls: Relevant business areas must assess and assure risks relating to financial settlement and reconciliation and are responsible for maintaining documented processes and procedures and deploying adequate monitoring and control to prevent and detect financial crime.	Chief Financial Officer	Ongoing
Risk Area	**Description of Risk**	**Minimum Control Standards**	**Who is responsible**	**When**
Financial settlement and reconciliation (continued)		Detective Control: Audit trails must be maintained so that system access can be monitored. To ensure that the Group's controls remain effective the Group undertakes internal audits to test and assess their effectiveness.	Chief Information Officer Internal Audit	Ongoing Ongoing
Criminal facilitation of tax evasion	Inadequate controls lead to Post Office failing to prevent criminal facilitation, by its associated persons (which includes employees, agents, clients, suppliers, contractors, etc.), of a UK or foreign criminal tax evasion	Preventative controls: Post Office ensures that guidance is issued to agents that they must comply with the Criminal Finances Act 2017 and Post Office's obligations and relevant clauses are included in all supplier contracts. Post Office has a Group wide training programme to ensure that all customer facing staff, back office staff and contractors receive adequate training. Staff and contractors are	Group Tax and Agents Development & Remuneration ~~All Employees~~	Ongoing Ongoing

Commented [SS20]: Amended to reflect CFA review and practice

POL00423570

		required to complete mandatory compliance training within 30 days of joining Post Office and annually. Detective Controls: Pass rate and number of test attempts is monitored to identify risk areas and any additional training or guidance required.	Human Resources are responsible for any incidents where further action is required and ensuring completion of mandatory training Financial Crime Team is responsible for reviewing training effectiveness	Ongoing
Internal Financial Crime/Fraud	Controls to deter, prevent and detect financial crime and fraud are not adequate to prevent crime by employees	Directive Control: Post Office has developed a Code of Business Standards and model behaviours that set out the expected standards for all employees and contractors – this is made available to all new and existing staff and reinforced in communications. Staff are also encouraged to report suspicions or actual wrong-doing to	Group Chief People Officer ~~HR Director~~ and General Counsel	Ongoing
Risk Area	**Description of Risk**	**Minimum Control Standards**	**Who is responsible**	**When**
Internal Financial Crime/Fraud (continued)		Grapevine or via the Whistleblowing reporting avenues Detective Controls: All reports received of or instances identified of internal fraud will be fully investigated and where appropriate, Post Office will prosecute individuals.	Head of Internal Audit and General Counsel Head of Internal Audit and General Counsel	Ongoing

Commented [SS21]: Changed title

POL00423570

2.5. Product and Service Risk Tools

~~**Compliance EngagementRisk Assessment Tool**~~

~~The Compliance EngagementRisk Assessment Tool has been created by the Financial Crime Team to assist Product Managers to determine the level of risk exposure and engagement required for new products and services. The Compliance EngagementRisk Assessment Tool takes into account inherent risks (e.g. payment method, channel, customer demographic etc), UK regulations and legislation and industry best practice.~~

~~The Compliance EngagementRisk Assessment Tool can be found here.~~

The Financial Crime Engagement Tool has been created by the Financial Crime Team and enables the Product Manager to provide the Financial Crime Team with key details about their project so that the team have an understanding of the financial crime risks posed and support the Product Manager with their project. The Compliance Engagement Tool takes into account inherent risks (e.g. payment method, channel, customer demographic etc.), UK regulations and legislation and industry best practice, enabling the Financial Crime Team to ensure that appropriate controls and product features are in place to mitigate the inherent risks and meet regulatory and legal requirements

The Risk Assessment Tool can be found here.

Commented [ML22]: Insert link

Product Information Pack

Product Management are responsible for keeping the Product Information Pack (PIP) up to date in line with any product changes. The purpose of the PIP is to provide an overview of the product or service, including customer/transactional journey, parties involved, any contractual responsibilities, monitoring and control requirements. It should consider the inherent risks the product is exposed to from a Group and customer perspective and the framework for the effective risk mitigation of the product.

Commented [ML23]: Added to define ownership

The existence of detailed operating policies, procedures and processes may be referred to throughout this document and is to be used to illustrate how the risks associated with the product are reduced.

The Product Information Pack can be found here.

11

POL00423570

3. Where to go for help

3.1. Additional Policies

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

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

3.2. How to raise a concern

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

- Discuss the matter fully with their Line Manager; or,
- Report their suspicions by telephoning Grapevine on GRO or,
- Report the matter directly to the Money Laundering Reporting Officer (MLRO)
- staff can contact the Post Office's Whistleblowing officer, Post Office General Counsel who can be contacted by email at: whistleblowing GRO or by telephone on: GRO
- the confidential Whistleblowing Speak Up service 'Ethicspoint' provided by Navex Global via telephone on GRO
- or via a secure on-line web portal: https://secure.ethicspoint.eu/domain/en/report_custom.asp?clientid=106826

3.3. Who to contact for more information

If you need further information about this policy or wish to report an issue in relation to this policy, please contact financial.crime GRO

POL00423570

4. Governance

4.1. Governance Responsibilities

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

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

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

The Board is responsible for setting the groups risk appetite.

POL00423570

5. Control

5.1. Policy Version

Date	Version	Updated by	Change Details
November 2016	1	Georgina Blair	Roll out of Final version
July 2017	1.3	Thomas Richmond	Final draft
July 2017	1.4	Sally Smith	POL R&CC approval
September 2017	2	Sally Smith	Final Version approved by ARC
October 2018	2.1	Sally Smith	Annual review and amends
October 2018	2.2	Sally Smith	POL R&CC approval
October 2018	2.3	Sally Smith	POL ARC approval
December 2018	2.4	Thomas Richmond	POMS ARC Approval
December 2018	3	Thomas Richmond	Final draft
September 2019	3.1	Sally Smith	Annual review and amends
September 2019	3.2	Sally Smith	POL R&CC approval
September 2019	4.0	Sally Smith	Final version approved by ARC's
April 2020	4.1	Sally Smith	Updated with new Speak Up service contact details
June 2020	4.2	Sally Smith	Annual review and amends

5.2. Policy Approval

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

Committee	Date Approved
POL RCC	3rd September 2019
POMS ARC	19th September 2019
POL ARC	23rd September 2019
Committee	**Date approved**
POL R&CC	
POL ARC	
POMS ARC	

Policy Sponsor: Group Director of Legal, Risk & Governance

Policy Owner: Director of Compliance

Policy Author: Head of Financial Crime

Next review: July 2021~~September 2020~~

11

Company Details

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

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

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

POL00423570

GROUP POLICIES

Anti-Money Laundering and Counter Terrorist Financing Policy

Version – V6.2

11

Chief Executive's Endorsement
The Post Office Group is committed to doing things correctly. Our Values and Behaviours represent the conduct we expect. This policy supports these to help us ensure that wherever possible use of Post Office systems and products for money laundering or terrorist financing is prevented, and the highest standards of financial crime prevention, detection and management are maintained.

POL00423570

1. Overview 3
1.1. Introduction by the Policy Owner 3
1.2. Purpose 3
1.3. Core Principles 3
1.4. Application 4
1.5. The Risk of Money Laundering and Terrorist Financing 4
1.6. Legislation 4
1.7. Offences 5
2. Risk Appetite and Minimum Control Standards ..... 6~~7~~
2.1. Risk Appetite ..... 6~~7~~
2.2. Risk Assessment ..... 6~~7~~
2.3. Policy Framework ..... 7~~8~~
2.4. Who must comply? ..... 7~~8~~
2.5. Minimum Control Standards ..... 7~~8~~
2.6. Product and Service Risk Tools ..... 18~~20~~
3. Where to go for help ..... 19~~22~~
3.1. Additional Policies ..... 19~~22~~
3.2. How to raise a concern ..... 19~~22~~
3.3. Who to contact for more information ..... 19~~22~~
4. Governance ..... 20~~23~~
4.1. Governance Responsibilities ..... 20~~23~~
5. Control ..... 21~~24~~
5.1. Policy Version ..... 21~~24~~
5.2. Policy Approval ..... 21~~24~~
Company Details ..... 21~~25~~

11

POL00423570

1. Overview

1.1. Introduction by the Policy Owner

The General Counsel has overall accountability to the Board of Directors for the design and monitoring of controls to prevent or deter Financial Crime which includes Anti Money Laundering (AML) and Counter Terrorist Financing (CTF). Financial Crime is an agenda item for the Audit and Risk committees and the Post Office Board is updated as required.

1.2. Purpose

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

Commented [SS1]: Definition updated to include 'employee' and 'staff'

1.3. Core Principles

Money Laundering and Terrorist Financing are criminal offences and everyone working in the business has a personal obligation to prevent them taking place and conduct business in accordance with applicable AML laws, rules and regulations set out by the business. The governance arrangements described in this Policy are based upon the following core principles:

- Post Office has devised a robust Policy and associated procedures (set out in this document) which are proportionate to the risks and complexity of the Group;
- The Group ensures that its policies reflect the principles of the AML and CTF regulations and legislation;
- The Group's overall and ongoing risk management process includes a risk based assessment of the financial crime risks to which the Group and its business are exposed, and the quality of its AML and CTF controls and monitoring;
- The Group undertakes a training and awareness program to ensure employees are aware of the risks of money laundering and terrorist financing, what they should do if they are suspicious, and the potential consequences should they fail to comply with the law;
- The Group promotes ethical and professional standards to prevent it from being used, intentionally or unintentionally by criminals;
- Decisions taken by management are consistent with the Board's approved strategic objectives and Risk Appetite;

Commented [EF2]: Word inserted to add clarity

11

[1] In this policy "Post Office" and "Group" mean Post Office Limited and any wholly owned subsidiary that formally adopts this policy~~Post Office Management Services Ltd~~.

[2] In this policy "employee" and "staff" means all persons working for the Group or on our behalf in any capacity including employees at all levels, directors, officers, agency workers, seconded workers, volunteers, interns, and contractors.~~In this policy "employee" means permanent staff, temporary including agency staff, contractors, consultants and anyone else working for or on behalf of Post Office.~~

POL00423570

- Every member of staff is responsible for understanding and managing the risks they take on behalf of the Group;
- Clear accountabilities are delegated by management to staff who have the right level of skill, competency and experience;
- All employees are required to comply with Group Policies.

1.4. Application

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

In exceptional circumstances, where risk sits outside of the Group's accepted Risk Appetite, a Risk Exception can be granted. Further information in relation to the risk exception process, together with a template can be found here

While Post Office does not tolerate events that are criminal in nature and which may give rise to unacceptable and illegal behaviour, it recognises that despite its many endeavours, it is not possible to eliminate all risk of Post Office being used to facilitate Money Laundering or Terrorist Financing activities, and therefore takes a risk based approach.

Failure to comply with the requirements of this policy by any employee will be regarded as a significant breach impacting on the Group's risk and control environment and may lead to disciplinary action up to and including dismissal and possible prosecution.

The risk to the Group in relation to Money Laundering and Terrorist Financing is reviewed by the Board as part of its wider commitment to Financial Crime on a regular basis.

1.5. The Risk of Money Laundering and Terrorist Financing

Money Laundering
Money laundering is the process criminals use to hide, disguise and dispose of cash and assets obtained from criminal activity. Criminals want to disguise the source of their money and remove any link to the original crime. This allows them to avoid prosecution and confiscation of funds.

Terrorist Financing
Terrorist financing involves dealing with money or property that may be used to fund terrorism. The funds and property may be from legitimate sources (e.g. personal funds, charities, sponsored trips, etc.) or criminal sources.

Failure to manage these risks can result in financial loss, customer impact, terrorism, regulatory breaches, fines, prosecution, prevention from selling a particular product, loss of existing or future contracts/relationships and damage to reputation.

11

1.6. Legislation

There are a number of relevant UK legal and regulatory requirements which are applicable including (but not limited to):

- The Money Laundering~~,~~ Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (known as Money Laundering Regulations 2017) amended by the Money Laundering and Terrorist Financing (amendment) regulations 2019.
- The Proceeds of Crime Act 2002
- The Criminal Finances Act 2017

Commented [EF3]: Wording inserted to reflect the change in legislation

POL00423570

- Policing and Crime Act 2017
- The Terrorism Act 2000
- Counter-Terrorism Act 2008

The Group monitors and takes into consideration guidance and other assistance offered by regulatory, industry and other specialist bodies, for example the Joint Money Laundering Steering Group (JMLSG), Wolfsberg Group, UK Finance (which incorporates BBA, UK Payments and Financial Fraud Action UL), Link, etc. publish trends and analysis on current threats and issues.

Oversight of compliance with the Money Laundering Regulations by the Group is undertaken by HMRC in the case of Post Office Limited and the Financial Conduct Authority (FCA) is the case of Post Office Management Services Limited (POMS).

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

1.7. Offences

The Money Laundering regulations set out five offences for which the Group or a member of its staff can be prosecuted under:

1. **Concealing** - where an employee conceals, disguises, converts or transfers criminal proceeds, or removes them from the UK
2. **Arrangement -** where an employee allows the Group to enter into or become involved in an arrangement where an employee knows or suspects that it involves the proceeds of crime.
3. **Acquisition, use or possession** - where an employee acquires, uses or takes possession of criminal proceeds.

   If found guilty of these offences an individual can be given an unlimited fine or up to 14 years in prison or both. The only defence is that an employee had completed and submitted a Suspicious Activity Report (SAR) to the Money Laundering Reporting Officer (MLRO), apart from 'acquisition' where the Group or a relevant individual would need to evidence that the proceeds had been acquired at fair market price and that they were not aware that they were criminal proceeds.
4. **Failure to disclose -** where an employee fails to report to the MLRO their suspicions or knowledge that someone is involved in Financial Crime.

   If found guilty of this offence an individual can be given an unlimited fine or up to five years in prison or both. There are two defences to this offence; training did not cover how to complete a SAR or "a reasonable excuse" such as that an employee was rushed to hospital just prior to completing the report. The reasonableness of the excuse will be tested in court.
5. **Tipping Off –** an offence will be committed if an employee discloses to a third person that a SAR has been made to a relevant authority and that said disclosure may prejudice any future investigation from the SAR. In addition an employee commits the offence if they disclose the fact that an investigation into a money laundering offence is being contemplated or carried out and the disclosure of this information is likely to prejudice this investigation~~formation~~. This information must have come to the employee in the course of business while in the regulated sector.

   If found guilty of this offence an individual can be given an unlimited fine or up to five years in prison or both. The only defence is if an employee did not know or suspect that what was said would prejudice the investigation.

Commented [EF4]: Correct wording added to reflect the offence

11

POL00423570

2. Risk Appetite and Minimum Control Standards

2.1. Risk Appetite

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

The Group takes its legal and regulatory responsibilities seriously and consequently has[3]:

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

The Group acknowledges however, that in certain scenarios even after extensive controls have been implemented, a product or transaction may still sit outside the agreed Risk Appetite. In this situation, a risk exception waiver will be required (See section 1.4 for further details).

2.2. Risk Assessment

The Money Laundering regulations require that Post Office completes Group wide risk assessments with a clear rationale to prevent and detect money laundering and terrorist financing.

Risk assessment must include:

- Identifying any inherent money laundering risks that are relevant to the Group, product and/or service
- Assessing customer type, customer behaviour, normal product/service activity, delivery channels, etc.
- Assessing controls to manage and reduce the impact of inherent risks
- Assessing how the Group will monitor controls and improve their efficiency
- Keeping records of key decisions

The Group requires risk assessments to be completed for individual products and services to ensure that sufficient controls are in place to detect and prevent money laundering or terrorist financing, and for these risk assessments to be refreshed at least annually for high risk products and services and where an issue is highlighted, significant risk is identified, an incident occurs or the regulations change.

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

POL00423570

2.3. Policy Framework

Post Office has established a suite of financial crime policies and procedures, on a risk sensitive approach which are subject to annual review. The policy suite is designed to combat money laundering, terrorist financing, bribery and corruption, fraud and ensure adherence to relevant sanctions regimes.

The Anti-Money Laundering and Counter Terrorist Financing Policy is a key Policy under the Financial Crime Policy framework and should be considered and read in conjunction with the overarching Financial Crime Policy and the Fit & Proper Policy where relevant.

2.4. Who must comply?

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

Where non-compliance is identified the matter must be referred to the MLRO. Any investigations will be carried out in accordance with the Investigations Policy. Where an instance of non-compliance is caused through wilful disregard or negligence, this will be treated as a disciplinary offence.

2.5. Minimum Control Standards

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

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

POL00423570

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
Oversight	Group does not comply with its AML/CTF regulatory responsibilities.	Directive Control: The regulations require a member of the Board of Directors or equivalent management body to be appointed as the officer responsible for overseeing compliance with regulations. For Post Office this is the General Counsel	General Counsel	Ongoing
		Preventative Control: The Group appoints an appropriate individual within the Compliance area as MLRO. With the assistance of the Financial Crime Team, the MLRO's main responsibilities include: • To receive reports of suspected money laundering or terrorist financing and to disclose to the NCA where required • Keep the Group up to date in relation to Financial Crime legislation • Putting in place and then monitoring compliance with the AML/CTF regime • Reporting to the ARC and R&CC all instances of non-compliance and any regulatory concerns or issues • Reporting to the regulators instances of non-compliance, where required	MLRO	Ongoing
		• Annual MLRO reports for the Board (for Post Office Management Services Limited and for Post Office Limited) covering: the governance framework; operation and effectiveness of the control framework (including documentation of policies and risk assessments); external threats/ landscape; summary of business issues and recommendations.	MLRO	Annual
		Corrective Control: Risk assessments must be undertaken at least annually for high risk products and services and where an issue is highlighted, significant risk is identified, an incident occurs or the regulations change.	MLRO	Issue, incident or change

POL00423570

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
Proposed product or service	Products, services or relationships with third parties may rely on systems or processes where prevention or detection of money laundering or terrorist financing has not been considered in the design, which may result in facilitation of laundering or terrorist financing leading to reputational damage and/or regulatory sanctions.	Preventative Control: As part of the design of a new product or service: • A Product Information Pack (see 2.6 below) must be completed and fully up to date. • Product or service risks must be considered and documented using the Financial Crime Engagement Tool (see 2.6 below). Prior to launch, the Product Information Pack (PIP) must be reviewed and approved by the Financial Crime Team. The Financial Crime Team adopts a risk based approach to determine when the full risk assessment should be completed, and the PIP will provide them with key information to make an informed decision. If the product is deemed high risk, the assessment will be completed prior to launch, following which the Financial Crime Team may require the Product Manager to make changes to reduce the risks prior to launch. The product manager/management team is responsible for ensuring their product complies with AML/CTF regulatory requirements.	Product Manager Financial Crime Team Product Manager	During design phase Prior to Launch Ongoing
Existing products and services	Due to changes in law, regulation, incidents, threats or practices over time, there is a risk that the controls to prevent and detect money laundering or	Preventative Control: Risk assessments must be undertaken at least annually for high risk products and services, where any changes to the product or service (including supplier changes) are made, where an issue is highlighted, significant risk is identified, an incident occurs, or the regulations change	Product Manager	Annually, or at any time there is a change

Commented [EF5]: Word inserted to reinforce control

Commented [EF6]: Words inserted to reinforce control

Commented [EF7]: Included to clarify first line responsibilities

POL00423570

	terrorist financing are no longer adequate.	The product manager/management team is responsible for ensuring their product complies with AML/CTF regulatory requirements. Prior to the scheduled risk assessment, the Product Information Pack (PIP) must be reviewed and updated by Product Management and provided to the Financial Crime Team. Prior to any product or service changes being implemented, the Product Information Pack (PIP) must be reviewed and updated by Product Management. The Financial Crime Team adopts a risk based approach to determine when the full risk assessment should be completed, and the PIP will provide them with key information to make an informed decision. If the product is deemed high risk, the assessment will be completed prior to change going live.	Product Manager Product Manager	OngoingAny time there is a change Ongoing
Risk Area	**Description of Risk**	**Minimum Control Standards**	**Who is responsible**	**When**
Existing products and services (continued)		Where no initial risk assessment was undertaken, product management must complete a new or update the existing Product Information pack and provide this to the Financial Crime Team. The Financial Crime Team will then agree a timescale to complete a risk assessment. Where the reassessed/assessed risk is considered by the Financial Crime Team to rest outside of the Group's Risk Appetite, or where the strength of the controls is deemed inadequate, as part of the Close Down report recommendations will be provided to the Product Manager to implement or improve controls to mitigate the risks. The Product Manager is responsible for producing an action plan outlining how these risks will be mitigated	Product Manager and Financial Crime Team Financial Crime Team and Product Manager	Any time there is a change Annually or Wwhen there is a material

Commented [EF8]: Included to clarify first line responsibilities

Commented [EF9]: Included to clarify requirements for scheduled risk assessments

Commented [SS10]: To reflect that Product Manager is responsible for updating PIP

Commented [EF11]: Updated to reflect our current process.

POL00423570

		and subsequently enacting the plan. Where risks cannot be sufficiently mitigated in line with the Group's risk appetite then the risk exception process must be followed. Corrective Control: Product Management must implement escalation procedures for when an incident is identified, so that the Financial Crime Team are made aware and if the product is outsourced to a third party, the third party is made aware. Product Management are responsible for addressing and overseeing any control failings to mitigate money laundering or terrorist financing risks. Risk assessment may be undertaken where an issue is highlighted by monitoring or an incident occurs that is deemed to be systemic.	Product Manager	issue or incident As and when
Financial settlement and reconciliation	Inadequate controls and audit trails relating to financial settlement and reconciliation may result in facilitation of laundering or terrorist financing leading to reputational damage and/or regulatory sanctions.	Preventative Controls: Relevant business areas must assess and assure risks relating to financial settlement and reconciliation and are responsible for maintaining documented processes and procedures and deploying adequate monitoring and control to prevent and detect money laundering or terrorist financing. Detective Control: Audit trails must be maintained so that system access can be monitored. To ensure that the Group's controls remain effective, the Group undertakes internal audits to test and assess their effectiveness, as agreed by the Board.	Chief Financial Officer Chief Information Officer Internal Audit	Ongoing Ongoing Ongoing
Monitoring	The Group fails to undertake adequate transaction monitoring	Preventative Control:	Product Manager/MLRO	Ongoing

Commented [EF12]: Updated to reflect our current process.

Commented [EF13]: New control to reinforce first line responsibility

Commented [SS14]: Amended to reflect current process

POL00423570

	and fails to prevent and detect money	Where the Group is directly regulated for products or services, sufficient transaction monitoring must be undertaken to ensure that suspicious activity, non-		
Risk Area	**Description of Risk**	**Minimum Control Standards**	**Who is responsible**	**When**
Monitoring (continued)	Laundering and terrorist financing.	Non-conformance and breaches can be identified, and provide assurance that customer data capture and due diligence thresholds have been set at a level commensurate with the risk exposure and to ensure compliance with money laundering regulations.		
Due Diligence	Group fails to undertake appropriate due diligence of a customer and fails to identify criminal activity.	Preventative Control: The Group takes a risk based approach and considers: • The product or service • Its intended customer market base and normal transaction activity • Any other risks relating to the product Detective Control: The extent to which the Group will gather due diligence information varies depending upon the risk that the product or service poses however must be considered when: • a business relationship is established with a customer • money laundering or terrorist financing is suspected • there are doubts about a customer's identification at the time of the transaction or from information obtained previously	Financial Crime Team/Product Manager Financial Crime Team/Product Manager	Annually, or at any time there is a change As required
Politically Exposed	Post Office fails to appropriately manage the risks associated with doing business with PEPs.	Preventative Control: All products and services are required to have in place identification procedures, commensurate with the underlying risk assessment to ensure that it can identify where the product and service is being used by a PEP. Where a product or service is maintained by a partner or	Product Manager	Ongoing

POL00423570

Persons (PEP)[4]				
Risk Area	**Description of Risk**	**Minimum Control Standards**	**Who is responsible**	**When**
Politically Exposed Persons (continued)		Third party, the obligations of the parties to identify a service user as a PEP must be documented and agreed. Determine the level of identification and assess if PEP checks are required. Detective Control: Ensure sufficient information is captured to undertake PEPs screening where deemed appropriate. Ensure controls in place to undertake Enhanced Due Diligence is required on any PEP relationship identified. Corrective Control: Where PEPs screening identifies PEPs, ensure that sufficient due diligence is undertaken to manage the risks.	Product Manager Product Manager Product Manager Product Manager/MLRO	Ongoing Ongoing Ongoing Ongoing
Sanctions[5]	The Group transacts with a customer who is sanctioned, resulting in the Group breaching international sanctions, reputational	Preventative Control: All products and services are required to have in place sufficient identification procedures, commensurate with the underlying risk assessment to ensure that the product and service is not used by a customer who is sanctioned.	Product Manager	Ongoing

[4] PEPs are those who have or are seen to have access to public influence and/or public money and as such are seen as being at higher risk of corruption. A PEP is someone who is: An individual who has or has been in a prominent public role in the UK or abroad such as Heads of State, MPs, Heads of Armed Forces, etc. An immediate family member or a known close associate of such as person.

[5] Sanctions are restrictions put in place by a government or a multilateral organisation (such as the United Nations) that limit a person, company or countries access to financial services or financial markets, funds or economic resources in order to achieve a specific foreign policy or national security objective.

POL00423570

	damage and/or regulatory sanctions.	Detective Control: Ensure sufficient information is captured to undertake Sanctions screening where deemed appropriate prior to a transaction occurring.	Product Manager	Ongoing
Risk Area	**Description of Risk**	**Minimum Control Standards**	**Who is responsible**	**When**
Sanctions (continued)		Corrective Control: Where screening identifies a transaction that maybe going to or from a sanctioned entity the Post Office will ensure that transactions are declined and the transaction is reported via SAR to the authorities. In the event that an employee becomes aware or suspects that a Sanctioned party is conducting business within the Group this must be reported immediately to the MLRO.	Product Manager/MLRO All employees	Ongoing Ongoing
Premises Registration	The Group fails to maintain up to date premises registration leading to penalties and sanctions. (The Group must maintain an up to date register of premises addresses that undertake directly regulated activity with HMRC – any changes must be registered and the relevant fees paid within 30 days)	Directive Control: Business rules must be agreed with HMRC in respect of the premises types that must be registered (e.g. Mobile Vans). Preventative Control: Premises registration business rules are reviewed annually and any potential changes to premises type are discussed and agreed with HMRC. Branch premises data is reviewed fortnightly and changes submitted to HMRC.	MLRO Financial Crime Team Data Centre of Excellence and Financial Crime Team	Ongoing Ongoing Fortnightly
Training	Through inadequate training, staff allow money laundering or	Preventative Control: Post Office has a Group wide training programme to ensure that all customer facing (branch) staff, back office	Financial Crime Team/HR/MLRO	Annual

POL00423570

	terrorist financing to take place, resulting in reputation damage and regulatory fines.	staff and contractors receive adequate training tailored to business risk areas. Product and marketing managers must ensure that any product training, promotions or communications are in line with AML & CTF policy and processes.	Product Manager	Ongoing
Risk Area	**Description of Risk**	**Minimum Control Standards**	**Who is responsible**	**When**
Training (continued)		Outsource providers, clients & suppliers must maintain records to evidence that staff have received adequate and regular training. New branch staff are required to complete AML/CTF training before they transact on Horizon, and back office staff and contractors within 30 days of joining. Detective Controls: Pass rate and number of test attempts is monitored to identify risk areas and any additional training or guidance required.	Product Manager/MLRO ~~HR~~The People Function Financial Crime Team	Ongoing Ongoing Ongoing
The MLRs require that impacted direct employees undertake the HMRC Fit & Proper test (Please see Fit & Proper Policy Standard for	Due to inadequate screening, there is a risk that key individuals involved in money service business are unfit to undertake a role.	Preventative Control: All Board members, GE, the MLRO and designated roles must pass the HMRC Fit & Proper test to ensure that the Group has employed individuals who are suitable to perform their roles. A register of completed and up to date Fit & Proper tests is maintained. Post Office completes pre-employment screening to ensure that an individual is fit and proper for their role. For further information please see the employee vetting policy.	MLRO People Director ~~of Human Resources~~	Within 30 days of appointment Pre-employment

Commented [EF15]: New Minimum Control Standard added to reinforce first line responsibility

Commented [SS16]: Changed title

Commented [SS17]: Change title

POL00423570

details of full controls)		Detective Control: The Group completes ongoing screening to ensure that an individual continues to remain fit and proper for their role.	People Director ~~Director of Human Resources~~	Ongoing where required
Risk Area	**Description of Risk**	**Minimum Control Standards**	**Who is responsible**	**When**
The MLRs require that impacted direct employees undertake the HMRC Fit & Proper test (Please see Fit & Proper Policy Standard for details of full controls)	Failure to ensure and evidence that those individuals operating Post Offices that are 'responsible persons' are 'fit and proper' to undertake Post Office regulated activity	Preventative Control: All agents and 'responsible persons' as defined by HMRC must complete on-boarding screening, vetting and training. Records must be maintained for the duration that the 'responsible person' is party to the contract between the agent and Post Office, and details provided to HMRC, as required. All impacted 'responsible persons' are required to complete an annual declaration that they meet the requirements of the fit and proper test	~~Group Human Resources Director~~Group Chief People Officer & MLRO Network Operations Director	Ongoing Ongoing
Record Keeping	Customer and transactional data is not retained resulting in the Group being unable to identify suspicious or out of character transactions, leading to the Group being used to launder money.	Preventative Control: For products and services where the Group is directly regulated, records must be kept of all transaction data and data obtained for the purpose of identification for a minimum of 5 years from the date of creation/transaction. The MLRO also ensures that documents relating to money laundering topics (e.g. files on suspicious activity reports and investigations) are maintained for a minimum of 5 years.	Product Managers MLRO	Ongoing Ongoing

Commented [SS18]: Change title

Commented [SS19]: Changed title

POL00423570

Suspicious Activity Reports ("SAR") and Reporting	Failure to report suspicions to the National Crime Agency[6] results in the	Preventative Control: The Group provides training to all employees, agents and agent assistants and provides easily accessible methods to report a suspicion to the MLRO and the Financial Crime Team.	All employees, agents and agent assistants	Ongoing
Risk Area	**Description of Risk**	**Minimum Control Standards**	**Who is responsible**	**When**
Suspicious Activity Reports ("SAR") and Reporting (continued)	Group being used to fund terrorism.	Where there are suspicions or concerns, the MLRO can apply to the NCA for a defence to money laundering or terrorist financing in regards to a specific transaction or set of transactions.[7]	MLRO	As required
		Corrective Control: Where issues are identified additional training and guidance is provided to increase employee understanding of the SAR regime.	Financial Crime Team	Ongoing
		Appropriate mechanisms are in place to protect Post Office and de-risk where concerns are identified relating to a specific individual or Group undertaking transactions in the Post Office network.	Financial Crime Team	Ongoing
		Detective Control: Where a SAR is not disclosed to NCA, it is reviewed and assessed by a senior manager, and the subject matter of the report is monitored for a minimum of three months to ensure that the appropriate decision was taken. Audit trails are maintained so that reports made can be monitored.	Financial Crime Team	Ongoing

[6] The NCA receives all SARs reported in the UK and their role is to investigate in conjunction with other intelligence. Where appropriate the NCA may provide copies of SARs to other intelligence bodies and investigation services (Law Enforcement, HMRC, etc.).

[7] Where defence is requested, this can take up to seven working days for the NCA to review and during this time customers must not be advised that defence is being applied for as this would constitute 'tipping off'.

POL00423570

2.6. Product and Service Risk Tools

Financial Crime Engagement Tool

The Financial Crime Engagement Tool has been created by the Financial Crime Team and enables the Product Manager to provide the Financial Crime Team with key details about their project so that the team have an understanding of the financial crime risks posed and support the Product Manager with their project. The Financial Crime Engagement Tool takes into account inherent risks (e.g. payment method, channel, customer demographic etc.), UK regulations and legislation and industry best practice, enabling the Financial Crime Team to ensure that appropriate controls and product features are in place to mitigate the inherent risks and meet regulatory and legal requirements.

Commented [EF20]: Updated to reflect the new assessment tool

The Risk Assessment Tool can be found here.

Product Information Pack

The purpose of the Product Information Pack (PIP) is to provide an overview of the product or service, including customer/transactional journey, parties involved, any contractual responsibilities, monitoring and control requirements. It should consider the inherent risks the product is exposed to from a Group and customer perspective and the framework for the effective risk mitigation of the product.

The existence of detailed operating policies, procedures and processes may be referred to throughout this document and is to be used to illustrate how the risks associated with the product are reduced.

The Product Information Pack can be found here.

POL00423570

3. Where to go for help

3.1. Additional Policies

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

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

3.2. How to raise a concern

Any Post Office employee who suspects that Post Offices products, services or processes have been used to facilitate money laundering, terrorist financing, or dishonest or fraudulent activity has a duty to:

- Discuss the matter fully with their Line Manager; or,
- Report their suspicions by telephoning Grapevine on GRO or,
- Report the matter directly to the Money Laundering Reporting Officer (MLRO)
- Staff can contact the Post Office's Whistleblowing Officer, Post Office General Counsel who can be contacted by email at: whistleblowing GRO or by telephone on: GRO
- the confidential Whistleblowing Speak Up service 'Ethicspoint' provided by Navex Global via telephone on: GRO
- or via a secure on-line web portal: https://secure.ethicspoint.eu/domain/en/report_custom.asp?clientid=106826

3.3. Who to contact for more information

If you need further information about this policy or wish to report an issue in relation to this policy, please contact financial.crime GRO

11

POL00423570

4. Governance

4.1. Governance Responsibilities

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

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

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

The Board is responsible for setting the Groups risk appetite.

POL00423570

5. Control

5.1. Policy Version

Date	Version	Updated by	Change Details
November 2016	3	Georgina Blair	Final Version approved by ARC
August 2017	3.1	Thomas Richmond	Version updated to reflect legislation changes
September 2017	3.2	Thomas Richmond	POL R&CC approval
September 2017	4.0	Sally Smith	Final Version approved by ARC
October 2018	4.1	Sally Smith	Annual review and update
October 2018	4.2	Sally Smith	POL R&CC approval
October 2018	4.3	Sally Smith	POL ARC approval
December 2018	4.4	Thomas Richmond	POMs ARC Approval
December 2018	5.0	Thomas Richmond	Final Version approval by ARC
September 2019	5.1	Sally Smith	Annual review and update
September 2019	5.2	Sally Smith	POL & POMS RCC Approval
September 2019	6.0	Sally Smith	Final version approved by ARC's
April 2020	6.1	Sally Smith	Updated with new Speak Up service contact details
June 2020	6.2	Sally Smith	Annual Review and update

5.2. Policy Approval

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

Committee	Date Approved
POL R&CC	**3rd September 2019**
POMS ARC	**19th September 2019**
POL ARC	**23rd September 2019**
Committe	**Date Approved**

Policy Sponsor: General Counsel/Group Director of Legal, Risk & Governance
Policy Owner: Head of Financial Crime
Policy Author: Head of Financial Crime
Next review: September 2019

Company Details

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

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

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

POL00423570

GROUP POLICIES

Document Retention and Disposal Policy

Version – V1.2

DRAFT

11

POL00423570

1. Contents

1. Contents....2
2. Overview....3
2.1. Introduction by the Policy Owner....3
2.2. Risk Appetite....3
2.3. Purpose....3
2.4. Core Principles....4
2.5. Application....4
2.6. Definitions....4
2.7. Legislation....5
2.8. Industry Guidance....6
3. Minimum Control Standards....7
4. Tools – Retention Schedules....13
4.1. Functional Retention Schedules....13
5. Where to go for help....14
5.1. Additional Policies....14
5.2. How to raise a concern....14
5.3. Who to contact for more information....14
6. Control....15
6.1. Policy Version....15
6.2. Policy Approval....15

DRAFT

POL00423570

2. Overview

2.1. Introduction by the Policy Owner

This policy sets out Post Office's commitment to the proper and lawful retention and disposal of its Information Assets by the Group. Information held for longer than is necessary carries additional risk and cost. Conversely, information not kept for long enough leaves Post Office vulnerable to knowledge or evidence gaps and sanctions from some of our regulators. Post Office recognises that failure to follow these principles will negatively impact business efficiency, and the ability to protect its interests as well as those of its customers and stakeholders.

2.2. Risk Appetite

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

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

- **Averse** risk appetite in relation to not complying with law and regulations or deviation from its business conduct standards, of which this standard forms part
- **Averse** risk appetite in relation to any serious impact to the confidentiality, integrity and availability of information, leading to financial loss, business disruption, public embarrassment or legal consequences in line with risk impacts
- **Tolerant** risk appetite for legal and regulatory risk in those limited circumstances where there are significant conflicting imperatives between conformance and commercial practicality
- **Averse** risk appetite for litigation in relation to high profile cases/ issues
- **Averse** risk appetite for data loss/ leakage that can lead to customer, commercial or reputational damage
- **Averse** risk appetite for inaccurate and unreliable processing of data
- **Averse** risk appetite for inefficient or ineffective or prolonged failure of, governance and control processes, critical financial reporting processes, critical supply chain and business continuity processes.

DRAFT

2.3. Purpose

The Document Retention and Disposal Policy is a cornerstone for good information management in Post Office. Information management supports the delivery of Post Office services in an efficient and accountable manner, helping to maintain its position as a trusted provider, retaining information for operational use while ensuring adherence to the laws and regulations concerning them. The objective of this policy is to ensure that the Group complies with its legal obligations in respect of the retention and disposal of Information Assets, keep important information for future use or reference, organise

POL00423570

information so it can be searched and accessed at a later date and dispose of information that is no longer needed.

This policy defines a set of high level principles to manage the retention and disposal of Post Office's information Assets in a timely and secure manner according to business needs and legal and regulatory requirements.

All Employees have a responsibility to understand the requirements set out in this policy and seek clarification from their line manager or the Departmental Data Steward in the case of any uncertainty. A list of Data Owners and Departmental Data Stewards will be maintained on the Data Management area of the intranet and will be updated when staff change, or new ones are added. The address for the Data Management Site is: https://poluk.sharepoint.com/sites/Extranet/FandO/DG/Lists/Entities/AllItems.aspx

2.4. Core Principles

Compliance with this policy will assist in meeting the following principles:

- Information that is needed to minimise the risk to Post Office from investigations, litigation or disputes will be easier to locate and will be retained systematically.
- Employees will have clear guidelines for the secure disposal of information, protecting against misuse and data breaches.
- Information that contributes to the Post Office's story in society will be protected, supporting corporate memory and brand identity through heritage.
- Post Office is subject to many laws and regulations which have information retention requirements. Compliance with these requirements will significantly reduce the risk of financial penalties, prosecution or reputational damage.
- Properly managed retention and disposal of information will allow Post Office to defend its actions by evidencing document destruction. Retention schedules and destruction/transfer documentation will underpin auditable disposal processes. In particular, this will support compliance with the Freedom of Information Act and the Data Protection Act 2018.
- Timely disposal of information will lead to financial savings for document storage, as well as day to day efficiency savings when retrieving information.

2.5. Application

This standard applies to all Post Office staff and third-party's who have access to Post Office data especially those with elevated rights to Post Office data.

2.6. Definitions

Data

'Data' is defined as the elements that form part of systems and processes that are created or pass through our systems.

Data Entity

'Data Entity' is the term used to describe a concept in a data repository that is a container of data & relationships to other objects – such as Branch, Customer, Employee, Product etc.

Data Owner

POL00423570

'Data Owner' is the person (usually GE or GE-1) who is accountable for a data entity (or multiple data entities).

Departmental Data Steward

'Departmental Data Steward' is the person allocated by a Data Owner to undertake the day to day processes associated with the controls required by the Data Owner.

Document Retention Schedule

'Document Retention Schedule' is the document detailing the various requirements of the data owner in regard to documents under their sphere of control.

Documents

'Documents' are specifically a type of information which has been used to form the basis of decisions, or to support business processes, in the normal day to day running of Post Office.

Employee

'Employee' means employees permanent employees, temporary including agency employees, contractors, consultants and anyone else working on behalf of Post Office.

Group

'Group' refers to Post Office Limited and its subsidiaries.

Information

'Information' is defined as a collection of data in the form of documents or other artefacts (such as spreadsheets, flow diagrams or reports) on which the business makes decisions.

Information Assets

'Information Assets' are collectively the Information, Data and Documents.

Structured Data

'Structured Data' has pre-defined data models or schema within a database or system file.

Unstructured Data

'Unstructured Data' consist all those that do not have pre-defined data models or schemas thus can't be so readily classified and fit into a neat box. Unstructured data files often include text and multimedia content: photos and graphic images, videos, webpages, PDF files, PowerPoint presentations, emails, blog entries, wikis and word processing documents.

2.7. Legislation

The following non-exhaustive list of legislation concerning the creation, management, disposal, use and re-use of documents and information is applicable to Post Office but please note that some legislation may be applicable only to some entities in the Group i.e. based on the services provided as at the date of this policy the Public Records Acts will only apply to Post Office Limited and not its subsidiaries (please note that the list below is not exhaustive and other legislation may apply):

- Postal Services Act 2000

POL00423570

- Data Protection Act (2018)
- Freedom of Information Act (2000)
- Companies Acts (1985, 2006)
- Limitation Act (1980)
- Public Records Acts (1958, 1967)
- Financial Services and Markets Act (2000)

2.8. Industry Guidance

This policy is based on the international standard for records management, ISO 15489 and the Code of Practice on the management of records under Section 46 of the Freedom of Information Act 2000.

DRAFT

POL00423570

3. Minimum Control Standards

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

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

At Document/System Creation

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
Product or service entity	Systems may not adequately support implementation of retention schedules and timely destruction of data. It may not be technically possible to permanently delete data or it may require a manual process.	As part of the design of a new product or service, or where a product or service is being updated, product or service risks must be considered, mitigated and documented before completion of design phase. This must include updating of any related Document Retention Schedules.	Product, Project and Programme Managers.	During design phase/ annually/ anytime there is a change
		The integrity and accuracy of data must be ensured at the point of collection.	Data Owner, Product, Project and Programme Managers.	During design phase/ annually/ anytime there is a change
Retention Schedules	Lack of creation or updating of retention schedules means that colleagues may not be aware of their obligations leading to inappropriate usage or retention of documents. This	Data Owners are responsible for maintenance and adherence of their retention schedules. All Data Owners must ensure that the retention schedules for their area are up to date. This is especially important when changes are being implemented to business processes.	Data Owner	All the time

DRAFT

POL00423570

	can cause Post Office to be fined or suffer reputational damage.			

During Use of a document or system

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
Risks to Information	Lack of understanding of the importance or sensitivity of the information flowing through a department could mean that employees do not perform the required actions on it.	Data Owners must ensure that all employees who view or process the information within their sphere of control understand the importance of that data.	Data Owners	Every 6 months in the Director assertions. All the time
		Data Owners need to understand the designs of systems or products such that they can fully understand the scope of their entity. Data Owners may pass this to Departmental Data Stewards, but they retain accountability.	Data Owners	All the time
		Data Owners must ensure evidence of any decisions are retained.	Data Owners	All the time
		Data Owners must understand the complete information lifecycle (creation, capture, index, manage, access, retrieve, administer, repurpose, share, retain, dispose, preserve) for all data within their sphere of control.	Data Owners	All the time
Access Control	Inadequate access controls may lead to unauthorised deletion of information including sensitive or business critical information.	Line Managers must assess and assure risks relating to employee access to systems and files, especially those containing sensitive or business critical data. All Systems must comply with the Access Control Standard.	Line Managers, Data Owners, Product, Project and Programme Managers.	All the time
Personal Data	Due to inadequate training, there is a risk of unintentional	Data Owners must ensure all employees within their areas understand their	Data Owners	All the time

DRAFT

POL00423570

	misuse of Personal Data, resulting in punitive penalties, reputational damage and a loss of licence to process personal data.	responsibilities in regard to the protection of personal data.		
		Data Protection must ensure that suitable training is made available to Data Owners and employees.	Data Protection	Annually
Employees	Due to inadequate training, there is a risk of under, or over, retention of information and failure to follow retention schedules, leading to punitive penalties or reputational damage.	All employees must undertake the annual Information Security and Data Protection training. They must also read and understand the Acceptable Use Standard, the Information Classification Standard and this document.	All employees	Annually/ within 3 weeks of starting
		3rd party suppliers must ensure that all employees with access to Post Office data and information undertake Post Office agreed information management training.	3rd party suppliers	Annually/ within 3 weeks of starting
		Ensure annual training contains adequate information on information management.	Data Owners	Annually
		Ensure the Policy Set contains adequate information on Information management.	Data Owners	Annually
Document Management	Failure to keep information evidencing appropriate destruction will increase time spent handling public access requests and will fail to protect Post Office in disputes around information rights regulations (such as Freedom of Information Act and Data Protection Act).	Data Owners must ensure that they have defined the storage requirements for the data under their sphere of control, and that this has been documented and agreed. This particularly applies where encryption is required. This is a field within the retention schedule.	Data Owners	Annually/when a change occurs
Retention Schedules	Lack of communication of required retention schedules may mean that incorrect decisions are made by	Data Owners must ensure that correct retention schedules are in place for the systems or product entities within their	Data Owners	Annually/ when a need is identified

POL00423570

	employees regarding information which could lead to regulatory fines or inability to answer a request to find or correct data.	sphere of control. These are required to be created at project initiation.		
		Line managers must ensure that they and all their employees are aware of the retention schedules in place for the data/information they process.	Line Managers	Annually/ when a need is identified
		Line Managers must remain aware of relevant regulatory and legislative requirements for document retention and must regularly review and update retention schedules in line with these as well as functional changes to their area.	Line Managers	Annually/ when a need is identified
Incident Management	Failure to understand the implications of an incident can lead to poor decision making or regulatory sanctions	Employees managing a incident must ensure that the relevant Data Owner is aware of any incidents to their data, and are satisfied with the resolutions.	Data Protection, Cyber Security Team, Physical security.	When an incident occurs
Processes and Procedures	Incorrect processes and procedures can lead to employees incorrectly using data.	Data Owners / Departmental Data Stewards are responsible for ensuring all processes which access the information within their sphere of control are adequate and appropriate.	Data Owners & Departmental Data Stewards	Annually / when a new process or procedure is written
Governance	Lack of governance over documents could lead to incorrect usage of data and thus result in fines or reputational damage to Post Office.	All employees implementing document management practices consistent with this Policy. Preserving documents as required under this Policy.	All employees	All the time
		Properly disposing of information at the end of its retention period.	All employees	All the time

POL00423570

		Monitoring compliance with this Policy.	Respective GE	All the time
		Educating employees in document management practices.	Head of MI, Analytics, Data Strategy, Data Protection and Cyber Team.	Annually
		Maintaining the repository of retention schedules.	Cyber Security	All the time
Legal/ Regulatory Framework	Failure to understand the requirements of any legal or regulatory issues by the Data Owner may lead to Post Office receiving sanctions where documents or entities have not been controlled appropriately	Ensure when creating their Document Retention Schedules all regulatory or legal requirements have been considered.	Data Owners	Annually

During Document/System Disposal

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
Risks to Information	Incorrectly disposing of information could mean that, through lack of continued controls being implemented for a defunct system/document, Post Office may suffer a data breach.	Data Owners must ensure that they enforce the clauses within a contract at the end of its term.	Data Owners	When a contract closes
		Data Owners must ensure that all users of the entities or documents under their sphere of control understand what actions are to be taken at the end of a retention period.	Data Owners	All the time

DRAFT

POL00423570

		All employees must ensure they understand what needs to be done with a document or system at the end of its retention period.	All Employees	All the time
Document Management	Failure to keep information evidencing appropriate destruction will increase time spent handling public access requests and will fail to protect Post Office in disputes around information rights regulations (such as Freedom of Information Act and Data Protection Act).	The Destruction or transfer of information must be authorised by the Data Owner or Departmental Data Steward and documented so that an audit trail exists.	All employees, Data Owners, Departmental Data Steward	All the time

DRAFT

POL00423570

4. Tools – Retention Schedules

Retention schedules will ensure that retention of information is considered prior to its creation. Some record types can be identified as having definite long-term business or historical value due to the activities they arise from. For others, their value may change over time, or an event (such as an audit or legal action) may require that their scheduled disposal is put on hold. All disposal of information must therefore be approved by the Data Owner before it is actioned and records must be reviewed where this is necessary to make a decision.

Disposal of information at the end of its assigned retention period means either destruction or transfer. Destruction of information must follow Post Office procedures as defined by the Data Owner / Departmental Data Steward in order to prevent a data breach (procedures apply to destruction of hard copy documents, electronic information and hardware). Where documents have been identified as suitable for transfer to The Postal Museum archive Departmental Data Stewards must ensure they comply. This should not be confused with transfer of semi-current or inactive documents to off-site storage facilities. Documents at the end of their retention period must not be transferred to off-site storage facilities unless they are subject to a hold on disposal.

Duplicate documents should be destroyed as soon as possible. Where information has been regularly shared between business units, only the original documents should be retained. Care should be taken that seemingly duplicate documents have not been annotated. Where Post Office shares information with other bodies, Post Office must ensure that they have adequate procedures in place so that the information is managed in accordance with the relevant legislation and regulatory guidance.

4.1. Functional Retention Schedules

Retention schedules set out the groups of documents that Post Office functions will maintain and when these are due for review, transfer to The Postal Museum or secure destruction.

Information on retention schedules will fall into three main categories:

1. Destroy after an agreed period – where the useful life of a group of documents can be easily pre-determined (for example, destroy 3 years after creation; destroy 6 years after the end of the financial year).

2. Automatically select for permanent preservation – where certain groups of documents can be readily defined as worthy of permanent preservation and transferred to The Postal Museum.

3. Review – examine documents to determine whether they should be destroyed, retained for a further period or transferred to The Postal Museum for permanent preservation. Documents which fall under category 1 may need to be reviewed for potential legal hold if they pertain to an active case.

Retention periods and actions are based on informational value, evidential value, legal or regulatory requirements, and historical value.

DRAFT

POL00423570

5. Where to go for help

5.1. Additional Policies

This guideline is one of a set of policies in respect of the use of Information by the Group. The full set of policies can be found at:

https://poluk.sharepoint.com/sites/cybersecurity2/SitePages/Cyber-and-Information-Security-Policy-Set.aspx

5.2. How to raise a concern

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

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

Post Office encourages members of the public or people not employed by us who suspect that this policy has not been complied with by a Post Office Employee to write, in confidence, to the **Chief Executive's Office, Finsbury Dials, 20 Finsbury St, London EC2 9AQ** or contact us at https://www.postoffice.co.uk/contact-us

5.3. Who to contact for more information

If you need further information about this policy or wish to report an issue in relation to this policy, please contact Cyber Security Team via cyber GRO

DRAFT

POL00423570

6. Control

6.1. Policy Version

Date	Version	Updated by	Change Details
26/02/2018	0.1	IPA & CoSec	First draft Version
04/03/2018	0.2	IPA & Head of MI, Analytics and Data Strategy	Edits following peer review.
07/03/2018	1.0	General Counsel	First Final Version
21/03/2018	1.1	IPA	Updated with minor comments after RCC
3/07/2020	1.2	Cyber Security	Updated to reflect the current policy structure

6.2. Policy Approval

Group Oversight Committee: Risk and Compliance Committee (RCC)
Sign-off Authority: Risk and Compliance Committee (RCC)
Policy Sponsor: Chief Information Officer
Policy Owner: Chief Information Security Officer
Policy Author: Ehtsham Ali
Approved by: Post Office Management Services Limited RCC
Post Office Ltd RCC

Approved: XX/07/2020
Next review: XX/07/2020

DRAFT

POL00423570

Policy *Procurement Policy*

Version – V0.2

11

POL00423570

1. Overview 3
1.1. Introduction by the Policy Owner 3
1.2. Purpose 3
1.3. Core Principles 3
1.4. Application 43
1.5. The Risk 43
1.6. Legislation 43
1.7. Industry Guidance 43
2. Risk Appetite and Minimum Control Standards 5
2.1. Risk Appetite 5
2.2. Policy Framework 5
2.3. Who must comply? 6
2.4. Minimum Control Standards 97
3. Tools & Definitions 118
3.1. Tools ..... Error! Bookmark not defined.8
3.2. Definitions 118
4. Where to go for help 129
4.1. Additional Policies 129
This Policy is one of a set of policies. The full set of policies can be found at: 129
https://poluk.sharepoint.com/sites/postoffice/Pages/policies.aspx 129
4.2. How to raise a concern 129
4.3. Who to contact for more information 129
5. Governance 1310
5.1. Governance Responsibilities 1310
6. Control 1411
6.1. Policy Version 1411
6.2. Policy Approval 1411
Company Details 1411

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

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

POL00423570

1. Overview

1.1. Introduction by the Policy Owner

The Procurement Director has overall accountability to the Board of Directors for the governance of procurement activities for goods and services.

Post Office spends about £500m per annum on goods and services from third parties. From an operational and commercial perspective, the management of this expenditure is critical in achieving commercial sustainability.

Compliance to the Procurement Policy is an agenda item for the Audit and Risk Committee and the Post Office board is updated as required.

1.2. Purpose

The purpose of this policy is to set out the way in which the Post Office will govern the procurement activities for goods and services.

It is one of a set of policies which provide a clear risk and governance framework and an effective system of internal control for the management of risk across the Post Office. Compliance with these policies supports the Post Office in meeting its business objectives and to balance the needs of shareholders, employees and other stakeholders.

1.3. Core Principles

Procurement shall be driven by the following Guiding Principles in all procurement activities:

Cost

- Achieve sustained value by progressively managing POLs expenditure, maximising value and seeking continuous improvement and innovation for the Post Office.

Contract

- To reduce risk to the Post Office by having contracts in place to ensure the delivery of goods and services to the agreed requirements, and to seek continuous improvement from the commercial relationships agreements.

Compliance

- To ensure the risk to The Post Office is minimised by having contracts and commercial arrangements in place to ensure delivery of goods and services to agreed requirements and to enable continuous improvement from our the relationships with suppliers

Consolidation

- Deliver efficiencies to The Post Office by managing the supply base to consolidate spend with onboarded strategic suppliers, and to reduce the total number of suppliers and contracts requiring direct management.

POL00423570

1.4. Application

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

The risk to the Group from Procurement is reviewed by the board annually.

In exceptional circumstances, where the procurement activity sits outside of the Post Office's accepted Risk Appetite a Risk Exception can be granted. For further information in relation to the risk exception process please contact the Risk & Assurance team – georgina.blair GRO

For definitions please see section 3.1.

The risk to the Post Office in relation to Procurement is reviewed by the board annually.

1.5. The Risk

The Procurement Policy is designed to establish best practice and mitigate the risk . All procurement activities shall adhere to the Post Office Procurement Policy. Procurement shall ensure that risk management is appropriately applied at all stages of procurement activities. Guidance shall be made available to enable the Procurement team to employ Post Offices risk management principles.

Procurement activities shall be properly planned and carried out in a manner that will enhance Post Offices capability to prevent, withstand and recover from interruption to the supply of goods and services where commercially viable.

1.6. Legislation

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

- Public Contract Regulation 2015 - Public Sector Procurement is subject to Public Contract Regulations ("PCR") 2015. PCR enables the public sector to focus on getting the right supplier in accordance with sound commercial practice and as a publicly funded organisation, we are mandated to comply with the regulations.
- Competition Act 1998
- Concession Contracts Regulation 2016
- Modern Slavery Act 2015

1.7. Industry Guidance

[*include an overview of any industry guidance or regulatory requirements that are relevant to this policy*]

POL00423570

2. Risk Appetite and Minimum Control Standards

2.1. Risk Appetite

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

The Post Office takes its legal and regulatory responsibilities seriously and consequently has:

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

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

2.2. Policy Framework

Post Office has established a suite of Procurement policies and procedures , on a risk sensitive approach which are subject to an annual review. The Policy suite is designed to assist with Supplier Management, Contractual Processes, and procurement exercises These have been developed to comply with applicable legislation and regulation and covers the following specifically:

Procurement shall be driven by the following Requirements in all procurement activities:

1. Supplier selection

- Selection and appointment of suppliers must be based on their ability to perform as defined as well as taking into consideration social values, ethical practices and environmental impacts. In particular this includes confirmation of the acceptance of our Supplier Code of Conduct and financial due diligence. This will be managed through our on-boarding and sourcing procedures;
- Post office staff do not enter into supplier selection, discussions with 3rd parties, make a commitment to spend, or undertake any procurement exercise without the involvement of the procurement team

2. Sourcing and Procurement exercises

- Must Contract on the best possible terms for POL, managing the balance between opportunity & risk, and utilising existing contract provision where appropriate to comply with legislation, in particular Public Contract Regulations (2015);
- Ensure that transparency and accessibility is embedded within our processes and activities, so that equal opportunities for small and medium sized businesses,

POL00423570

minority owned businesses, social enterprises and the voluntary and community sector will be provided;
- Ensure that the aims of the business on diversity, sustainability and other aspects of corporate social responsibility are embedded within our processes and activities

3. Managing Contractual Processes
- Manage the POLs contracting process in accordance with internal policy and external legislation,
- Ensuring that Contracts address the key issues. These include defining vendor expectations, performance, scope of work, and deliverables. In particular, confirmation should be sought regarding understanding of and adherence to the following POL policies: Bribery and Corruption, Tax Evasion, Confidentiality and Health and Safety. All contracts must protect our physical and intellectual property and data and, in the interests of transparency, include a right of audit;
- Ensure a managed handover of agreements for contract management by the business, and any ongoing responsibilities for the resolution of issues raised in accordance with the contract.
- Post office staff must not enter into any material contractual changes without the involvement of the procurement team, such as a change of scope or value outside what was originally advertised in the procurement exercise.

4. Managing Suppliers
- Support Contract Managers in the business as they respond to performance issues and monitor suppliers, to ensure that the supply chain risk is managed and disputes are resolved.
- Ensure there is a defined governance structure in place to manage strategic and core suppliers so that there is a mechanism to escalate issues, to influence their priorities to align with ours, and to achieve a sustainable service through continuity planning.

5. Managing Risk
- Understand the risks and complexities of the goods and services we procure to segment the supply base into tiers to identify the strategic, critical and core suppliers, and to conduct risk analysis on specific threats.
- Having contracts in place with suppliers that will mitigate risk and enable the monitoring of improvement over time.
- Working with Contract Managers to ensure that the business has adequate arrangements in place with critical suppliers for supply disruption, business continuity and disaster recovery.

The principles of contract, performance and relationship management will be covered separately in the Supplier Relationship Management Policy (PP3)

The principles of transactional Purchasing (Purchase to Pay (PP2) and the use of Corporate Purchase Cards (PP4) are addressed in their own respective policies.

2.3. Who must comply?

This policy applies to all employees who procure from suppliers. Compliance with this policy is mandatory for all business units within POL. PayZone does not currently fall within these business units but may do so in future.

In the case of agencies and consultancies, all contracted personnel working on behalf of POL shall be made aware of this policy and shall comply with all procurement procedures listed within the Procurement department guidance.

POL00423570

All employees who procure from suppliers should work to our values Care, Challenge and Commit and our standards set out in the Code of Business Standards and the other POL policies listed in 4.1. All staff working on behalf of POL should not enter into supplier selection, discussions with 3rd party, commitment to spend, material contractual changes or any procurement exercise without the involvement of the procurement team.

This policy does not apply directly to outsourced service providers or to suppliers; however, by making sure that suppliers comply with our Supplier Code of Conduct it does seek to ensure our outsourced service providers and suppliers must: support the governance of POL; mitigate the risks faced by POL; and support the quality of service we provide to our customers, our policies and other legal requirements (including finance, health and safety, human rights and labour standards, and employment laws);

****

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

2.4. Roles & Responsibilities

Procurement shall drive the procurement process, negotiate commercial arrangements, and support the means by which procured solutions are delivered.

Procurement Director is responsible for:

- Administering this policy on behalf of the CEO
- Developing and rolling out the supporting strategies to drive continual performance improvement.

Procurement Department is responsible for:

- Driving, adopting and sharing best practice procurement and sourcing standards and initiatives;
- Developing category strategies and
- Creating compliant procurements exercises and contracts with adequate contract handover to Contract/ Vendor Managers to deliver
- Developing mutually beneficial collaborative trading relationships with suppliers;
- Monitoring the evaluation and assessment of suppliers' supply practices (including ethical, sustainable measures), taking appropriate commercial action as necessary.

Contract/ Vendor Managers are responsible for:

- Monitoring the evaluation and assessment of suppliers' supply practices (including ethical, sustainable measures), taking appropriate commercial action as necessary.

Directorate/Business Managing Directors are responsible for:

- Ensuring that this policy, supporting procedures and corrective actions are implemented and complied with; and
- Leading by example in protecting the POL brand and championing knowledge sharing across the divisions.

Managers are responsible for:

- Implementing and enforcing the processes and procedures;
- Ensuring that their people are aware of their responsibilities and receive appropriate training.

Suppliers are responsible for:

POL00423570

- Acting in accordance with this policy and associated procedures and guidance provided in their contracts and the Supplier Code of Conduct.

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

POL00423570

2.5. Minimum Control Standards

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

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

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
Activities of employees and consultants	Failure to ensure that Consultants and Employees comply with the Post Procurement Policy and supporting procedures	**Preventative Control** All procurement activities shall adhere to the Post Office Procurement Policy. Procurement shall ensure that risk management is appropriately applied at all stages of procurement activities. Guidance shall be made available to enable the Procurement team to employ POLs risk management principles.	Procurement Director	Ongoing
Procurement activity	Failure to uphold good practise procurement principles	Procurement activities shall be properly planned and carried out in a manner that will enhance POLs capability to prevent, withstand and recover from interruption to the supply of goods and services where commercially viable.	Procurement Team	Ongoing
Data Input	Maintenance of accurate data input within the eProcurement systems to monitor compliance.	Compliance shall be collated periodically using spend and sourcing analytics extracted from POLs eSourcing and eProcurement systems, the Risk Committee reporting, and issues reported by the relevant category leads and line managers. It shall be the responsibility of the line managers to deal with the instances of non-compliance within their category teams and raise any disciplinary actions	Procurement Managers	Ongoing

POL00423570

Conflict of Interest	Failure to manage conflicts of interest related procurement	**Preventative Control** During procurement activity, conflicts of interest declarations are issued and reviewed. Any conflicts of interest risks are mitigated and recorded. Suppliers are contracted to comply with anti-bribery and corruption laws.	Procurement Director	Ongoing
Supplier Conduct	Reputational and commercial risk from poor supplier conduct	Effective due diligence of the supply base with additional risk based assessments and monitoring against Supplier Code of Conduct	Procurement Team	Ongoing
Vulnerable Customers	Customers not being able to access our branches, products or services.	During the tendering application the needs of vulnerable customers should be considered at the start of the process. This is captured via in-depth supplier questionnaires and supporting documentation.	Procurement Team	Ongoing

Post Office Limited - Risk and Compliance Committee-13/07/20

POL00423570

3. Definitions

3.1. Tools

1. **Web3** Source to Settle system - Sourcing and Contract Management through to Purchase to Pay modules

3.2. Definitions

1. **POL** – Post Office Limited entities and subsidiaries
2. **Post Office Insurance** – the Post Office Insurance business which is separate from the POL in regard to public subsidy.
3. **PCR** – Public Contract Regulations 2015 are rules on the procedures for procurement by contracting authorities with respect to public contracts.
4. **PRA** - Prudential Regulatory Authority is part of the Bank of England, promotes the safety and soundness of insurers, and the protection of policyholders
5. **FCA** - Financial Conduct Authority regulates how insurance firms behave, as well as more broadly the integrity of the UK's financial markets
6. **Material contractual change** – change of scope/ value outside what it was advertised for.

POL00423570

4. Where to go for help

4.1. Additional Policies

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

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

4.2. How to raise a concern

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

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

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

4.3. Who to contact for more information

If you need further information about this policy or wish to report an issue in relation to this policy, please contact the Procurement Director.

POL00423570

5. Governance

5.1. Governance Responsibilities

The Policy sponsor, responsible for overseeing this Policy is the Procurement Director of Post Office Limited.

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

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

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

POL00423570

6. Control

6.1. Policy Version

Date	Version	Updated by	Change Details
	0.1		Draft Version
09/06/2020	0.2	Susan Godfrey	Draft Version

6.2. Policy Approval

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

Committee	Date Approved
POL R&CC	
POMS R&CC	
POL ARC	
POMS ARC	

Policy Sponsor: Group Chief Finance Officer

Policy Owner: Procurement Director

Policy Author: Procurement Performance & Operations Manager

Next review: 30/06/2021

Company Details

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

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

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

POL00423570

POST OFFICE LIMITED

Meeting:	Audit, Risk & Compliance Committee
Date:	27 July 2020
Time:	14.30 - 17.00
Location:	1.19 Wakefield, Finsbury Dials, 20 Finsbury Street, London, EC2Y 9AQ / Microsoft Teams

Present:	**Invited Attendees:**
Carla Stent (Chair)	Amanda Bowe (Post Office Insurance ARC Chair): Item 2
Ken McCall (SID)	Jeff Smyth (Interim Group CIO): Item 4
Tom Cooper (NED, UKGI)	Tony Jowett (CISO): Item 4
Zarin Patel (NED)	Tim Armit (Business Continuity Manager): Item 5
Regular Attendees:	Maxine Cross (Head of Reward and Pensions): Item 6
Tim Parker (Chairman, POL)	Tim Perkins (Head of Security, Safety & Loss Prevention): Item 7
Alisdair Cameron (Group CFO)	Sarah Gray (Group Legal Director): Item 8
Ben Foat (Group General Counsel)	Barbara Brannon (Procurement Director): Item 9
Andrew Paynter (Audit Partner, PwC)	Amanda Jones (Group Retail and Franchise Network Director, Interim): Item 12
Stewart Light (Audit Director, PwC)	James Scutt (Head of Customer Experience): Item 12
Rosie Clifton (Audit Manager, PwC)	Sally Smith (MLRO & Head of Financial Crime): Item 12
Johann Appel (Head of Internal Audit)	
Mark Baldock (Head of Risk)	
Jonathan Hill (Compliance Director)	
David Parry (Senior Assistant Company Secretary)	

Join Microsoft Teams Meeting
GRO United Kingdom, London (Toll)
Conference ID: GRO
Pin (if applicable): GRO

Time		Item		Owner	Action
14.30	1.	Welcome & Conflicts of Interest		Chair	Noting
14.35	2.	Update from Subsidiaries: Post Office Management Services (ARC)		Amanda Bowe	Discussion & Noting
14.40	3.	Previous Meetings		Chair	Approval
		3.1	Minutes (19 May 2020; 16 June 2020)		
		3.2	Action List		
		3.3	Draft Risk and Compliance Committee Minutes (13 July 2020)		
14.45	4.	PCI-DSS and Cyber Security Update		Jeff Smyth/ Tony Jowett	Noting
		4.1	PCI-DSS	Jeff Smyth	
		4.2	Cyber Security	Tony Jowett	
		4.3	Joiners, Movers, Leavers	Tony Jowett	
15.00	5.	Business Continuity Update and Business Continuity Policy		Tim Armit	Noting
15.10	6.	Pensions Assurance – RM Pensions		Maxine Cross	Noting

12

Strictly Confidential

POL00423570

POST OFFICE LIMITED

15.25	7.	Suspense Accounts		Tim Perkins/ Ben Foat	Discussion & Noting
15.40	8.	Law & Trends Update		Sarah Gray/ Ben Foat	Noting
15.50	9.	Procurement Governance & Compliance Report		Barbara Brannon	Noting
16.00	10.	Consolidated Report from Risk, Compliance and Internal Audit			
16.00		10.1	Risk Report	Mark Baldock	Noting
16.10		10.2	Compliance Report	Jonathan Hill	Noting
16.20		10.3	Internal Audit Report	Johann Appel	Noting
16.30	11.	GDPR Update		Jonathan Hill	Noting
16.40	12.	Policies for Approval		Jonathan Hill	Approval
		12.1	Modern Slavery Statement	Amanda Jones/ James Scutt	Recommend for Board approval
		12.2	Business Continuity Policy		
		12.3	Anti-Bribery and Corruption Policy	Sally Smith	
		12.4	Whistleblowing Policy	Sally Smith	
		12.5	Financial Crime Policy		
		12.6	Anti-Money Laundering and Counter Terrorist Financing Policy		
		12.7	Procurement Policy		
16.55	13.	Any other business		All	Noting
Next ARC Meeting: Tuesday 22 September 2020 at 09.00 to 11.30 in 1.19 Wakefield, Finsbury Dials, 20 Finsbury Street, London, EC2Y 9AQ					

12