POL00423684

Audit, Risk and Compliance Committee Agenda

Date:	Monday 25 November 2019	Time	16.00 – 18.20 hrs	Location	1.19 Wakefield

Present	Other Attendees
• Carla Stent (Chair) • Tom Cooper • Ken McCall **Apology:** Tim Franklin	• Nigel Boardman - Observer (Audit and Risk Assurance Committee Chair, BEIS) • Nick Read (CEO) • Alisdair Cameron (CFO) • Ben Foat (General Counsel) • Andrew Paynter (Audit Partner, PwC) • Stewart Light - via telephone (Audit Director, PwC) • Sarah Allen (Audit Senior Manager, PwC) • Rosie Clifton (Audit Manager, PwC) • Johann Appel (Head of Internal Audit) • Jenny Ellwood (Risk Director) • Paul Beaumont (Head of Financial Services Regulation and Compliance) • Tom Lee (Head of Finance, Financial Accounting and Controls) • David Parry (Senior Assistant Company Secretary) • Edward Dutton (item 2.) (Interim Managing Director PO Insurance) • Shikha Hornsey (items 4, 8.) (Group CIO) • Tony Jowett (item 4.) (Chief Information Security Officer) • Sherrill Taggert (item 5.) (Legal Director (Interim) • Amanda Jones (item 7) (Retail Director) • Karl Oliver (item 7) (Head of Commercial Partnerships) • Lisa Cherry (items 9) (Group HR Director, Interim) • Mark Baldock - Observer (Head of Change Risk and Assurance)

	Agenda Item	Action Needed	Lead	Timings
1.	**Welcome and Conflicts of Interest**	Noting	Chair	16.00 – 16.05
2.	**Update from Subsidiaries:** • Post Office Management Services ARC (Verbal)	Noting & Input	Edward Dutton	16.05 – 16.10
3. 3.1 3.2 3.3 3.4	**Minutes and Matters Arising** Minutes of the Audit, Risk and Compliance meeting held on 23 September 2019 Actions List Actions List – update paper from DR testing in October Draft Minutes of the Risk and Compliance Committee held on 7 November 2019	Approval Noting & Input Noting & Input Noting	Chair	16.10 – 16.15
4.	**Cyber Security Update**	Noting & Input	Shikha Hornsey/ Tony Jowett	16.15 – 16.25
5.	**Contract Management**	Noting & Input	Ben Foat/ Sherrill Taggert	16.25 – 16.35
6.	**Designation as an "Accountable Person"**	Noting & Input	Al Cameron	16.35 – 16.45

POL00423684

Audit, Risk and Compliance Committee Agenda

7.	**Commercial Partner Contingency Paper (McColls)**	Noting & Input	Amanda Jones/ Karl Oliver	16.45 – 17.00
8.	**Consolidated Report from Risk, Compliance, and Internal Audit Departments**	Noting & Input		17.00 – 17.30
8.1	Risk Report		Jenny Ellwood	17.00 – 17.10
8.2	Compliance Report		Paul Beaumont	17.10 – 17.20
8.3	Internal Audit Report		Johann Appel/Shikha Hornsey	17.20 – 17.30
9.	**Policies for Approval**	Noting & Approval		17.30 – 17.40
9.1	Cover paper: • Change Management Policy • Protecting Personal Data Policy			
9.2	Cover paper: • Risk Policy		Jenny Ellwood	
10.	**Pension Scheme Controls**	Noting & Input	Lisa Cherry	17.40 – 17.50
11.	**UK Data Protection Act (including GDPR) Compliance Status Report**	Noting & Input	Paul Beaumont	17.50 – 18.00
12.	**POL Audit Strategy Memorandum 2020**	Noting & Input	Andrew Paynter	18.00 – 18.15
13.	**ARC Meeting Dates 2020 - 2021**	Noting	David Parry	18.15 – 18.20
14.	**Any other Business** Notes: • Date of next meeting 28 January 2020, 09.30 – 12.00 hrs.	Noting	Chair	

POL00423684

POST OFFICE LIMITED AUDIT AND RISK COMMITTEE MEETING
Strictly Confidential

3.1

MINUTES OF A MEETING OF THE AUDIT AND RISK COMMITTEE OF POST OFFICE LIMITED HELD ON MONDAY 23 SEPTEMBER 2019 AT 20 FINSBURY STREET, LONDON EC2Y 9AQ AT 08.00 AM

Present:	Carla Stent	Chair **(CS)**
	Tim Franklin	Non-Executive Director **(TF)** (items 5-15)
	Tom Cooper	Non-Executive Director **(TC)**
	Ken McCall	Senior Independent Director **(KM)**
In Attendance:	Nick Read	Chief Executive Officer **(NR)**
	Alisdair Cameron	Chief Finance and Operations Officer **(AC)**
	Tim Parker	Chairman, PO Limited **(TP)**
	Andrew Paynter	Group Audit Partner, PwC **(AP)**
	Rosie Clifton	Group Audit Manager, PwC **(RC)**
	Ben Foat	General Counsel **(BF)**
	Johann Appel	Head of Internal Audit **(JA)**
	Jenny Ellwood	Risk Director **(JE)**
	Jonathan Hill	Compliance Director **(JH)**
	David Parry	Senior Assistant Company Secretary **(DP)**
	Shikha Hornsey	Group Chief Information Officer **(SH)**
	Ben Cooke	IT Operations Director (item 4) **(BC)**
	Phey Rasulian	Programme Manager Payment Services, Retail **(PR)** (item 5)
	Tony Jowett	Chief Information Security Officer **(TJ)** (item 5)
	Dan Zinner	Chief Transformation Officer **(DZ)** (item 6) by telephone
	Mark Dixon	Head of Treasury, Tax & Insurance **(MD)** (item 8)
	Andy Bear	Account Manager, Locktons **(AB)** (item 8)
	Amanda Jones	Retail Director **(AJ)** (items 10, 11, 12)
	James Scutt	Head of Customer Experience, Retail **(JS)** (Item 10)
	Andrew Kingham	Head of Network, Retail **(AK)** (item 11)
	Karl Oliver	Head of Commercial Partnerships, Retail **(KO)** (item 12)
Apologies:		

Action

1. Welcome and Conflicts of Interest

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

2. Update from Subsidiaries

The Chair provided a quick overview of the key issues discussed at recent Post Office Insurance (POI) Audit and Risk Committee meeting of 18 September:

- There is a need to focus on the quality of sales and to embed good sales practices making them sustainable in the longer term. Training and the use of technology is key to this.
- Clarity has been received from Insurers regarding how travel policies will operate post Brexit.
- The Senior Manager and Certification regime is effective from 9 December 2019. The programme is on track and has been subject to an independent quality review by Ernst and Young who had highlighted no material issues.
- The Committee received training from the POL CISO team on cyber security to gain a better understanding of cyber risks and how they are controlled.

POL00423684

- The Committee also received a deep-dive on travel complaints plus a comprehensive update on financial crime.

3. Minutes and Matters Arising

3.1 The minutes of the meeting of the Audit and Risk Committee held on 23rd July were **APPROVED** and **AUTHORISED** for signature by the Chairman.

3.2 The minutes of the meeting of the Audit and Risk Committee held on 29th July were **APPROVED** and **AUTHORISED** for signature by the Chairman subject to minor amendments.

3.3 Progress with the completion of actions as shown on the action log was **NOTED**.

3.4 The draft minutes of the Risk and Compliance Committee held on 3 September 2019 were **NOTED**.

4. Belfast Data Centre Disaster Recovery testing lessons learned

4.1 The paper was taken as read.

4.2 BC reported the disaster recovery ('DR') training testing over the August bank holiday weekend could be considered successful considering that there had been limited testing since 2013. It was noted a number of issues regarding network connectivity had been identified whilst Horizon was running on the secondary server which the team was investigating. No issues with trading had been identified.

4.3 In order to keep momentum going, he suggested the following dates should be considered as potential dates for further testing:

- Full test May bank holiday weekend 2020;
- Full test over Christmas;
- Partial DR test on the weekend of 12th/ 13th October, with a full test in May 2020.

4.4 The Committee **AGREED** a partial test should be completed in October (weekend 12th/13th) followed by a full test in May 2020, with the management team assessing if an earlier full test over the Easter period was possible . (It was acknowledged that Christmas is POL's busiest period and therefore not advisable to conduct a full DR test). **Action: BC**

4.5 The Committee also **APPROVED** SH's request for an additional secondary data link. She advised it would be an unacceptable risk should the second server fail. **To do: SH**

5. PCI-DSS Update and Cyber Security Update

5.1 **PCI-DSS**

The paper was taken as read.

5.2 The Committee questioned the levels of progress made and noted that although no definitive plan regarding the banking solution had been committed to, a detailed design plan was expected at the end of October.

5.3 Findings from the recent feasibility study had identified no credible alternative supplier capable of processing both retail and banking transactions at a reduced cost whilst also accelerating the compliance programme.

5.4 The Committee discussed and sought to understand the following:

- Who the accountable GE member was.
- Whether compliance could be accelerated by sending POL staff on secondment to Ingenico.

POL00423684

- Ways to motivate Ingenico to treat the programme as a priority. Ingenico had advised that compliance would be completed in 2021, rather than 2020 as requested by POL.

5.5 The following points were noted. SH was the accountable GE member. There had been repeated high level conversations with Ingenico to motivate and prioritise compliance but without the desired effect. Additionally the team was unsure whether sending POL staff on secondment to Ingenico would accelerate compliance.

5.6 In view of the Committee's lack of confidence that compliance would be completed by December 2020 (as repeatedly reiterated to Ingenico), the following was **AGREED**: **Action:**

- NR would hold CEO talks with Ingenico's CEO. **NR**
- TC would hold talks with his French counterparts. **TC**
- An update including commercial figures would be presented at the October Board meeting.

5.7 The Committee noted the residual risk remained unchanged but that all parties were being kept informed of the progress of current status.

5.8 **Cyber Security**

The paper was taken as read.

5.9 All key Deloitte recommendations had now been completed and maturity was still on track for March 2020.

5.10 Recorded Futures (RF, POL's Cyber Threat Intelligence supplier) and the Security Operations Centre had been instrumental in helping to reduce cyber-attacks including 30 alerts that POL would not have previously been able to identify.

5.11 *Risk Appetite statement*

JE explained that following a review of the existing 2015 data risk appetite, a new Cyber Security Statement had been developed to reflect the current threat risk status. The statement is intended to be more easily interpreted by POL in the decision making process by recognising that some data types do not require to be managed with an 'averse' risk appetite.

5.12 She advised that the Harm table (used to assess impact and probability score) had also been reviewed to enable POL to understand what 'Averse' translated to – an 'averse' appetite means POL maintains a 'Green' risk target score for the compromise or loss of personal sensitive data. A 'neutral' appetite is adopted for data that does not contain Personal/Sensitive or Business Critical Information. The Committee noted the Harm table and congratulated the team on devising an easily understandable framework.

5.13 *Capital One data breach*

TJ reported he had met with the UK CISO of Capital One (who provide credit cards for POL customers) following a data hack in the USA. It was noted no POL customers had been affected.

5.14 The Chair noted the good progress made to date and thanked the team for their work.

6. Transformation Office Changes

6.1 The paper was taken as read.

6.2 DZ joined the meeting by telephone. He explained current focus was on centralising the Change programme; identifying suitable resource for the team; encouraging his team to challenge earlier in the process; to use centralised governance processes and to plan ahead.

POL00423684

6.3 It was noted the programme was split into eight change portfolios, these being: Retail Products, Telecom and Identity Products; Financial Services Products; Network Development; E2E Agent Relationships; IT Platform Enablement; LRG & Organisational Effectiveness; and Efficient Central Support. Capex exceptional spend was GRO and regular monthly updates are provided to UKGI.

6.4 TC commented on the change in approach and sought to understand the current position with DZ. He noted that there was an additional GRO of funding that had not been claimed, which AC advised related to the 5 year plan and would be drawn down in due course.

6.5 The Committee commented on the large number of programmes currently in train (170 programmes; mapped to the 8 change portfolios) and felt it would be appropriate to consider the prioritisation of the change portfolio at the POL Board. A further update on the change control environment would be presented to the ARC in January 2020. **Action: DZ**

7. Consolidated Report from Risk, Compliance and Internal Audit departments

7.1 **Risk**

The report was taken as read.

7.2 JE presented an update on POL's current risk profile. The following key risks were discussed: IT Technology & Interruption; PCI Compliance; Information Security Transformation Programme; Telecoms; and Brexit.

7.3 *IT Technology & Interruption*

JE advised the risk had increased from 'Amber' to 'Red' due to the following: key IT suppliers not performing required disaster recovery testing (DR) within the last 12 months along with the continued use of outdated software; Computacenter's current recovery time objective is outside of its contractually obliged response time; Verzion had deferred DR testing several times this year. A remediation plan is being agreed.

7.4 *PCI Compliance*

PCI-Compliance remains a key risk due to the lack of tangible progress made (as discussed earlier). No credible alternative providers have been found to Ingenico (capable of processing banking and retail transactions) and a detailed design plan is still outstanding.

7.5 *Information Security Transformation Programme*

All ten key recommendations from the Deloitte cyber maturity assessment have now been completed and cyber security is improving.

7.6 *Telecoms*

A separate update would be provided by JH, however a watching brief in relation to Telecoms was in place.

7.7 *Brexit*

Planning and regular meetings with BEIS for a 'no deal' exit continue. Effort is focused on the required changes for Mails and the possible additional support required for key branches.

7.8 Other risk areas of note included:

- Barclays Bank have advised that the commercial pricing for Banking Framework 2 is unacceptable and will cease cash withdrawals through POL branches from January 2020.

GRO

POL00423684

- A comprehensive risk workshop was held in July with Payzone, to develop their risk register and to align their risk framework to POL's.
- The implementation of Archer Risk and Control application continues. 'Go live' is expected in November once user acceptance testing and training for the central risk team has been completed in September and October respectively. Roll out is expected to take place within 3-6 months.

7.9 **Compliance**

The report was taken as read.

7.10 JH highlighted the following key compliance issues.

7.11 *Text Relay*
Ofcom had requested further information to evidence when senior managers had been informed of non-compliance. A meeting with Ofcom is scheduled for Tuesday 24 September to discuss findings. Whilst JH expected POL to be penalised, the regulator had recognised POL's transparency in this matter.

7.12 *GDPR*
The team was in the process of remediating original contracts to be GDPR compliant. It is expected this project would be completed by March 2020.

7.13 *Fit & Proper*
The Declaration Oversight Committee met in August to formally agree to switch off non-compliant branches following repeated notifications. There are 294 branches currently who have not provided information. Since August, 478 branches were switched off, 148 of which were switched back on following receipt of information required. One commercial partner was yet to provide details.

7.14 The Committee recommended that (if not already completed) Area Managers visit all branches in their patch to re-iterate the importance of completing fit and proper returns. Further, the National Federation of Sub-Postmaster (NSFP) should also be contacted to advise members of the importance of completing their returns. To do: AJ

7.15 TC sought and received confirmation that stock would be returned to POL where branches had been switched off.

7.16 *External Threats – banking deposits*
The Committee noted the increased number of high value complex banking deposits made at POL branches and later determined to be associated with criminal activity. The total amounted to c.£65 million and all reasonable steps were being taken to identify these transactions and to work with the authorities and the relevant banks.

7.17 Whilst POL was not liable for money laundering, the Committee was fully aware of the reputational and regulatory scrutiny that POL could potentially face. Work was underway to mitigate/reduce these risks with area managers and NSFP being made aware of the impact.

7.18 **Internal Audit**
The report was taken as read.

POL00423684

7.19 JA advised the IA plan for 2019/2020 was progressing well. He expected nine audits to be presented at the next ARC meeting in November. The Chair requested these be circulated to the Committee should they be completed before the next meeting in November. To do: JA

7.20 Following a request to discuss a late paper, the Chair reminded the Executive that late papers not tabled with sufficient time for consideration would be discussed at a later date.

7.21 The Committee noted the Master Services Agreement between POL and Payzone Bill Payments Limited had now been signed.

8. Corporate Insurance Renewal 2019/20

The paper was taken as read.

8.1 MD presented the insurance renewal programme for 2019/20 (renewal is GRO GRO). He expected costs to be broadly in line with last year's programme at GRO but noted that renewal quotes for Crime Insurance and Directors' and Officers' Liability Insurance could only be provided GRO Approval was sought for the CFOO to finalise any matters that did not require the Committee's input.

8.2 GRO

GRO coverage for the remainder insurances remained similar to last year.

8.3 TC noted this was the first year an OJEU-compliant procurement programme had been completed and reminded the Committee of the commercial risks of not being compliant. (OJEU is the Official Journal of the European Union which is home to all public sector contracts over a certain value.) TC requested a future ARC review into the Procure to Pay processes. To do: DP

8.4 Following detailed discussion of the insurance renewal, the Committee **APPROVED**:

- The 2019/20 insurance renewal programme; and
- For delegated authority to be provided to the CFOO (Al Cameron) to finalise any matters not requiring ARC input, subject to a maximum spend of GRO

9. Policies for Approval

9.1 The following policies were **APPROVED:**

- Contract Execution Policy
- Financial Crime Policy
- Anti-Money Laundering and Counter Terrorist Financing Policy (includes the HMRC Fit & Proper Standards Policy)
- Physical Security Policy
- Vulnerable Customer Policy.

10. Modern Slavery

10.1 The paper was taken as read.

10.2 AJ and JS presented a revised statement that highlighted the key work completed this year including: raising awareness across the supply base and within the agency network; improved due diligence whilst on boarding new suppliers; and educating field teams and the network teams to spot signs of slavery.

10.3 Increased focus for 2019/20 would be spent on continuing to implement work from 2018/19 but would also include reviewing guidance presented to Post Masters to ensure a consistent message and guidance was traversed across the Group, suppliers and network.

POL00423684

10.4 The Committee discussed in-depth the risks of managing oversight across the network and the supply network, and recommended that practical information brochures / training / communications should be prepared for all branches and Post Masters to support them understand the issues being faced. Further, awareness should be raised with the NFSP.

10.5 Following an in-depth discussion of the issues (and confirmation from the external auditors that this was the most comprehensive debate that they had attended on the matter), the Committee **RECOMMENDED** that the 2019/20 Modern Slavery Statement be approved by the Board.

10.6 The Committee requested the auditors to review/consider the modern slavery practices of similar sized and structured clients to see whether there are any areas of best practice that can be considered. **To do: PwC**

11. Deep Dive: Quality of Financial Services Sales in the Network.

11.1 The paper was taken as read.

11.2 The Committee received a presentation from AJ and AK on the Quality of Financial Sales in the Network, following a decline in mystery shopping results. (All firms regulated by the FCA (Post Office Insurance, Bank of Ireland and Capital One) are subject to oversight and supervision for any financial services or products distributed and sold.)

11.3 AK remarked that customer relationship managers (CRMs) introduce and sell products to customers using tablets and are video mystery shopped on Savings and Life Insurance. Although miss-selling, pressure sales, cancellations and complaints are low, the mystery shopping results had indicated that sales conversion is poor, which in turn could lead to poor customer outcomes and the customer not being treated fairly.

11.4 Following a strategic change in focus to support and train CRMs in August, JH remarked that results were beginning to improve. A team of dedicated Area Managers was now responsible for training staff.

11.5 The Committee discussed the simple use of technology to sell products and advised that if not already done so, mandatory training should be provided for all those involved in selling financial services products.

11.6 TP commented on, not withstanding current technology constraints, the need for, and benefits and competitive advantage of having, accurate and current MI data to understand the levels of sales at branches and to identify where funding and resource was required.

11.7 The Chair thanked the team for their work to date.

12. Deep Dive: Monitoring of Multiple Retail Partners

12.1 The paper was taken as read.

12.2 The Committee received a presentation from AJ and KO on Monitoring of Multiple Retail Partners. Since May, the team had been engaged with Risk, BEIS and the Finance and Commercial team to develop a resilience tracker to review key retail partners for any signs of financial distress. Where signs of distress have been flagged, a financial review of partner performance is completed.

12.3 KO observed that following a recent review, McColls had been flagged as partner of concern and that contingency planning had been implemented. Although McColls had opened 40 new locations in the last 12 months, trading conditions had been difficult.

POL00423684

12.4 The Committee recognised the value of the tracker but sought to understand the triggers used for 'amber' and 'red' alerts (judgement call) and recommended that if not already doing so, credit insurance reports should be reviewed.

12.5 In order to understand future funding needs, the Committee requested further detailed modelling to understand the implications of a commercial partner going into financial recovery measures, and of an administrator selling branches. Consideration should also be given as to whether the number of branches owned by a commercial partner or franchisee should be capped. The Committee requested that a full contingency review of any partner flagged as having a red status be conducted. It was agreed that the contingency plan for McColls be shared with the Committee. **Action** AJ

13. Deep Dive: Financial Controls

13.1 The paper was taken as read.

13.2 AC remarked on the increased number of controls and improved first and second lines of defence within the financial reporting controls framework, but noted reconciliation issues remained between the cash management system and the cash centre finance software. Rectification was expected by the end of November.

13.3 KM raised concern that the number of manual processes and the difficulty with reconciliations could impact POL's financial figures. AC assured the Committee that controls exist for areas with a materiality in excess of £500k and that plans are in place to automate as many of the process as possible. A system was in place to track any reconciliation issues and the process should be rectified by the end of November.

13.4 The Committee noted the progress (albeit slow), recommended that new software be considered as per the recent IA report and to automate as many controls as possible.

14. Provision of External Auditor Consulting Services

14.1 The paper was taken as read.

14.2 The Committee noted that POL was currently refreshing its management consulting panel in line with CCS Framework RM3745. Since being appointed as external auditor, PwC's consultancy work had been limited. (The framework provides management consultancy advice for central government, arms-length bodies, non-departmental public bodies and the wider public sector, and allows for up-to 20 companies to bid for specific work.)

14.3 AP advised that PwC had been invited to join the panel, but before spending time on the tender, he wanted to understand the Committee's appetite for such engagements. It was noted that listed companies are required to have a ceiling of 70% non-audit fees : audit fees (non-audit fees cannot be higher than 70% of the average of the last 3 years audit fees), whereas there is no such requirement for non-listed entities. If applied at POL, this would equate to a fixed cap rate of £400K for non-audit fees.

14.4 The Chair noted the member's opinions and following a robust discussion, and in recognition that POL mirrored the corporate governance code as used by listed companies, the Chair **AGREED** that PwC would be allowed to bid (should they wish) but that the cap of £400K would be introduced for non-audit fees.

15. AOB

15.1 The Chair reminded the Committee that the next meeting would be attended by the BEIS ARAC Chair.

15.2 There being no further business, the meeting was closed.

POL00423684

POST OFFICE LIMITED AUDIT AND RISK COMMITTEE MEETING
Strictly Confidential

.....
Chairman **Date**

Actions from meeting

Minute	Action	Lead	Due Date
4.4 Belfast Data Centre Recovery Testing	The Committee **AGREED** a partial test should be completed in October (weekend 12th/13th) followed by a full test in May 2020, with the management team assessing if an earlier full test over the Easter period was possible .	BC	Oct.
5.6 PCI-DSS	NR to hold talks with CEO of Ingenico to progress PCI compliance.	NR	Oct.
5.6 PCI-DSS	TC to hold talks with his French counterparts to progress PCI compliance.	TC	Oct.
5.6 PCI-DSS	An update including commercial figures would be presented at the October Board meeting.	SH/PR	Oct.
6.5 Transformation	The Committee commented on the large number of programmes currently in train (170 programmes; mapped to the 8 change portfolios) and felt it would be appropriate to consider the prioritisation of the change portfolio at the POL Board.	DZ	Jan. 2020
12.5 McColls	To circulate contingency plan for McColls.	AJ	Oct.

POL00423684

REF.	ACTION	ACTION OWNER	DUE DATE	STATUS	OPEN / CLOSED
23 September 2019					
4. Belfast Data Centre Disaster Recovery testing lessons learned					
4.4	A partial DR test to be completed in October (weekend 12th/13th) followed by a full test in May 2020.	**BC**	November	Testing successful. Separate report provided.	Recommend for closure.
5. PCI-DSS					
5.6	NR to hold talks with CEO of Ingenico to progress PCI compliance.	**NR**	November	There has been a change of leadership at Ingenico and talks are ongoing to arrange CEO talks.	Open
6. Transformation Office Changes					
6.5	Consider the prioritisation of the change portfolio at the POL Board	**DZ**	January 2020	To be included in January Board agenda.	Open
12. Monitoring of Multiple Retail Partners					
12.5	Contingency plan for McColls to be circulated.	**AJ**	November	November ARC agenda item on contingency planning for multiple retail partners in distress.	Recommend for closure.
29 January 2019					
6. Money Laundering Reporting Officer (MLRO) Annual Report					
6. (a)	To provide regular updates on the complete fit and proper data to HMRC.	**Nick Boden/ Sally Smith**	Ongoing	**Ongoing until project close.** Item included on ARC agenda.	Open
7. Security Strategy					
7. (a)	To provide quarterly reports to the ARC showing how we were performing against the metrics agreed to implement the Security Strategy once the deep dive with Deloitte had taken place.	**Rob Houghton / Mick Mitchell**	May 2019	**Ongoing.** Item included on ARC forward agenda.	Open
9. Audit Strategy Memorandum	To consider a deep dive on Successfactors given the cost of the system and its limited functionality.	**Exec**	~~May 2019~~ July 2019	Proposals for deep dives and the sequencing of these will be brought to the May ARC meeting. Proposals will now be brought to the July ARC meeting.	Open

POL00423684

POST OFFICE LIMITED
AUDIT, RISK AND COMPLIANCE COMMITTEE

Belfast Datacentre Disaster Recovery Exercise

3.3

Author: Craig Bibby Sponsor: Shikha Hornsey Meeting date: 25 November 2019

Executive Summary

Context

The Fujitsu operated Belfast datacentre hosts Horizon our Post Office counter trading application, and other business critical applications. The resilience of this datacentre was successfully tested on the 12th October 2019 for the first time in six years. This partial DR (Disaster Recovery) test was performed during one night on a normal trading weekend to specifically test the connectivity and features which had failed in the previous DR test during the August Bank Holiday. This targeted, incremental testing of the datacentres has allowed us to significantly reduce business risk before the peak trading period and has enabled us to fulfil our obligations to clients and partners for this year.

Questions addressed in this report

1. How did the failover test in October go?
2. How has our risk position changed?
3. What are our next steps?

Conclusion

1. The test was a success and an important step in ensuring we can continue to trade in the event of a major failure in our primary datacentre. All major services were made available to the network and tested. We can now be sure that in the event of a disaster in our primary datacentre our business would be able to continue trading by failing over to our secondary datacentre. Some minor services failed testing initially, and whilst the issue was quickly diagnosed, there was not sufficient time to retest without interrupting morning trading. These are in the process of being addressed and will be re-tested again when we have the next annual DR test.
2. Our risk position has significantly improved, in the event of a live DR scenario in our environment we have a high degree of confidence in our ability to restore the Horizon application and continue trading. However, full performance during a day's trading and the replication of that day's trading data on failback to primary remain outstanding as they were out of scope of this partial test
3. Changes have been made to remediate the issues faced with minor services, we plan to conduct an isolated test on these in Jan 2020. Next year we plan to perform a full DR test in May 2020 over a bank holiday weekend, including full performance during a day's trading and the replication of that day's trading data. At this point we will have returned to our repeatable BAU exercise.

Input Sought

Noting paper only.

POL00423684

The Report

How did the failover test in October go?

All pre-test activities were completed successfully in the build up to the exercise, with one minor hardware issue reported and quickly resolved, culminating in a GO decision on Friday 11th October. Test environments were then shut down and baseline testing performed, the exercise commenced at 17:55 Saturday 12th October.

Time	Objective	Result
Saturday 17:55	Stop all PO Data Gateway (PODG) services	Successful
Saturday 18:00	Commence controlled shutdown of primary datacentre and MasterCard disconnect	Successful
Saturday 19:15	Horizon Online production service shut down, commencing fail over	Successful
Saturday 21:15	Starting production services in DR data centre	Successful
Saturday 22:20	MasterCard to implement LINK reconnect	Successful
Saturday 22:30 – 01:20	Restoration of network banking, counter services and model office validation testing. All major services tested, a number of minor 3rd party services unavailable.	All major services available and tested. Decision to fix forward and failback at 01:25 (25 of 30 complete)
Saturday 23:00	Fujitsu & Accenture perform isolated PODG test	Successful
Sunday 00:00	PODG test complete	Successful
Sunday 00:15	Decision point to review success of validation testing and monitoring, one hour until failback.	Successful
Sunday 01:20	MasterCard to implement LINK disconnect	Successful
Sunday 01:25	Confirmation of failback started	Successful
Sunday 05:00	Starting production services in primary data centre	Successful
Sunday 05:00	MasterCard to implement LINK reconnect	Successful
Sunday 05:00	Restoration of network banking, counter services and initiation of model office testing	Successful
Sunday 06:00	Third party confirmation testing	Successful
Sunday 06:15	Post failback, service availability check	Successful
Sunday 07:00	Automated Payment Client file delivery has commenced	Successful
Sunday 07:15	Accenture confirm file deliveries	Successful
Sunday 11:00	Accenture confirm files available in Arrow	Successful
Sunday 14:05	Fujitsu - All failover activities complete, systems and support are now handed back to BAU	Successful
Sunday 17:00	Back office and data processing UAT complete	Successful

POL00423684

WHAT WENT WELL?

There were a number of significant milestones achieved and activities completed that give us confidence in any future test.

- All major services were made available to the branch network and tested successfully in the secondary datacentre including Horizon counters, mails, network banking, PO Card Account, Identity services and Self Service Kiosks.
- Live branch traffic showed 73% of counters were online and connected to the secondary datacentre, with 141 unique branches transacting between 22:00 and 01:20 on the night of the 12th October.
- Services were restored 57 minutes ahead of schedule at 05:03 Sunday with all services fully tested before 6am Sunday.
- Fujitsu's revised technical plan was robust with learnings from the test in August and subsequent remediation's incorporated, this exercise plan will be formalised and available to be used in future if required.
- Building on the success of the August test, 16 Post Office staff were directly involved across the weekend, carrying out key testing and validation, and proving the Post Offices ability to support this test.

WHAT DIDN'T GO WELL?

Technical and organisational improvements have been identified, with remediation plans detailed below. There is also a number of lower level technical improvements detailed within the exercise report in appendix 1.

Issue	Description / Resolution / Action	Status
Technical		
GWS (General Web Services)	➢ GWS services allow a Postmaster to provide 3rd party information or a quote to a Customer, some of these services were unreachable during the test. This was caused by routing configuration which did not allow the services to be restarted outside of normal trading hours. ➢ An operational change has been implemented to routing configuration to resolve the issue. ➢ An isolated test script is currently being drafted, to allow these minor services to be tested without the need for a full DR.	Change made to rectify, plan to perform isolated test to confirm in Jan 2020

POL00423684

Communications		
Client Engagement	➢ Three clients raised incidents for file delivery delays, all of these were expected outcomes but the client's operational teams did not follow the agreed process. ➢ Each incident was resolved in due course and feedback given to the client operations teams. ➢ Client Relationship Managers for HSBC, Santander and GlobalPay to review communication with clients.	Complete
Planning & Execution		
Cash on Hand data issue	➢ An unexpected issue was seen in the Cash on Hand data, this was caused by branches making declarations between 18:00 and 19:00 on 12/10/2019. ➢ Communications to branches will specifically mention that declarations are not available during the test and an additional test will be incorporated to validate data on failback. ➢ Capture in lessons learnt and update communication plan.	Improvement action for next test

Has our risk position changed?

BUSINESS CONTINUITY

Overall we perceive the risk to our business continuity has significantly reduced, all mitigations to the residual risk are in planning and will be implemented through Change Mgmt. The risk score has been reduced from high (20) to medium (6).

Positive changes to risk position		Unchanged or negative changes to risk position	
All hardware and application's successfully running in the secondary datacentre	↓	Full days trading volume in secondary datacentre not tested.	→
Counter connectivity and live branch traffic tested successfully.	↓		
All major services tested in model office and the network.	↓	Data replication of full days trading from secondary back to primary datacentre not tested.	→
Across the business and key partners the planned approach is well understood.	↓		

POL00423684

What are our recommended next steps?

We have met our obligation to partners and clients in successfully testing the resilience of our core trading platform for this annual period. We will now work to remediate the untested services at the next opportunity, produce a further revised plan and schedule a regular annual test, 22nd – 25th May 2020. Key next steps are listed below;

1. **GWS (General Web Services) isolated test**

A Change has been implemented for 3rd party routing outside of normal business hours to allow a DR invocation at any time. Perform isolated test of GWS application and services, to resolve the issue and incorporate into future DR plan.

2. **Conduct a full DR test in May 2020**

The proposed test will be performed over the bank holiday weekend 22nd – 25th May 2020, including a full day's trading in the secondary datacentre and replication of that trading data back to the primary datacentre. Given the success of the test in October we have a high degree of confidence in our ability to perform this test.

In conducting the test successfully in May 2020, we will mitigate all identified risks associated with performing a DR test and invoking a live DR Failover. This will reduce the risk to low (4), achieving the current target risk score.

<table>
<tr><th colspan="2">Positive changes to risk position</th><th colspan="2">Unchanged or negative changes to risk position</th></tr>
<tr><td>All hardware and application's successfully running in the secondary datacentre</td><td>↓</td><td rowspan="2">Full days trading volume in secondary datacentre tested, load testing all hardware and applications</td><td rowspan="2">↓</td></tr>
<tr><td>Counter connectivity and live branch traffic tested successfully.</td><td>↓</td></tr>
<tr><td>All major services tested in model office and the network.</td><td>↓</td><td rowspan="2">Data replication of full days trading from secondary back to primary datacentre baselined and DR plan complete.</td><td rowspan="2">↓</td></tr>
<tr><td>Across the business and key partners the planned approach is well understood.</td><td>↓</td></tr>
</table>

POL00423684

3.4

POST OFFICE LIMITED RISK AND COMPLIANCE COMMITTEE
Minutes of a Risk and Compliance ("RCC") meeting held at
Finsbury Dials, 20 Finsbury Street, London EC2Y 9AQ
on 7 November 2019 at 13.00 pm

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

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

1.1 AC opened the meeting. He requested papers be shortened, the minutes summarised, and advised that papers would be taken as read.

1.2 The Directors declared that they had no new conflicts of interest in the matters to be considered at the meeting in accordance with the requirements of section 177 of the Companies Act 2006 and the Company's Articles of Association.

2. Minutes and Action Lists

2.1 The minutes of the RCC meeting held 3 September were **APPROVED**.

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

3. Supplier Contracts out of Governance

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

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

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

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

3.5 The Chair reminded the Committee of POL's obligation to adhere to the Public Contract Regulations 2015 and requested the requirement for tighter controls on contracts management be re-iterated in team meetings.

4. PCI-DSS Update

POL00423684

4.1	SH advised that she had met with Ingenico in Paris, where they had expressed their challenges in dealing with the bespoke product POL required. She expected to receive final pricing and deadlines at the end of this week (08/11/2019) which would be circulated.	**Action: SH**
4.2	Due to the devices in the field requiring a software update once the software had been accredited by QCS (Quality Control Systems), she did not expect compliance to be completed until Q1 2021. The software update would take a day at most to complete.	
4.3	The Committee noted POL's bespoke solutions but advised the report should more clearly articulate the reason for the extension in compliance. It was noted that the banks and ARC had been advised compliance would be in December 2020.	
5.	**Cyber Security**	
5.1	TJ reported he was relatively comfortable with the progress made in implementing the Deloitte audit recommendations, of the improved cyber security, and the improved approach to joiners movers and leavers. He had concerns with 3rd party disaster recovery testing and the culture of ineffective password controls being used on personal laptops, PCs and devices.	
5.2	He advised he would like to test maturity with POL's systems and 3rd party vendors by completing a major incident test such as a ransomware attack.	
5.3	The following was **AGREED**:	**Action:**
	1. Letters of discipline be sent to staff who do not improve their password security on PCs/laptops/devices.	**LC**
	2. A major incident test be completed with findings reported to the Committee.	**TJ**
	3. Joiners/movers/leavers – to review whether contractors who no longer work for POL have been removed from POL emails and systems.	**DZ/LC**
	4. Joiners/movers/leavers - A routine cycle of checking third party access to be implemented.	**TJ**
	5. Joiners/movers/leavers - IA to review end to end process of joiners/mover/leavers.	**JA**
6.	**Combined Risk, Compliance and Audit Update**	
	Risk	
6.1	The top risks of PCI, IT Technology and Interruption, People, Business Continuity, Payzone and Brexit were noted. The following points were discussed.	
6.2	**Payzone** (paragraph 1.6 of the report) - CM (as a Board member of Payzone) remarked that Payzone was happy with the risk framework/controls now in place and noted that Payzone had a dedicated POL risk partner.	
6.3	**PCI Compliance** (paragraph 1.3 of the report) – the project remained "Red" overall against current plan. SH agreed with this observation.	
6.4	**IDS Digital Identity** (paragraph 1.16 of the report) – the project is six months behind schedule [post meeting note JE – this is nine months behind schedule]. AC requested the wording be reviewed and questioned whether the project should be reviewed at the Investment Committee.	
	Compliance	
6.5	The following points were raised:	
6.6	**Review of Cookie approach** (paragraph 2.9 of the report) – recent ICO guidelines advised that companies could no longer rely on implied consent when placing ccokies on websites. JH advised this would reduce POL's ability to use customer data held. Expressed consent must now be given.	
6.7	**National Lottery and scratch cards** (paragraph 2.26) – tighter controls have been introduced by the Gambling Commission regarding the sale of gambling products to vulnerable customers. An agreed approach with the National Lottery is required.	
6.8	**Mystery Shopping** (paragraphs 2.33 – 2.34 of the report) – results continued to be poor, a stronger message to non-compliant sites is required. AC sought ways to improve standards.	**Action: JH**
6.9	**Super Complaint** – AC sought and received an update of the current position. Pricing papers would be presented to GE in December and were being reviewed against Ofcom's fairness principles.	
6.10	The Law and Trends forum continued to horizon scan for any legal/regulatory updates that may affect POL.	
	Internal Audit	
6.11	The following points were raised:	
6.12	**Purchase to Pay** – controls around POL spend management have improved, but it is still heavily manual and requires an upgrade.	
6.13	**Payzone Control Environment –** the control environment has improved over the last year and is for purpose, however when looked at overall, the control environment "needs improvement".	

DRAFT

POL00423684

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

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

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

7. Contract Management

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

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

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

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

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

8. Accountable Person

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

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

9. Accounting Overview

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

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

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

10. GDPR

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

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

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

11. Policies for Approval

11.1 The following policies were recommended for Approval at ARC:

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

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

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

13. Future meeting dates RCC and ARC 2020 - 2021

13.1 The meeting dates were noted.

The next scheduled RCC meeting is 14 January 2020.

14. Any other Business

There was no other business.

DRAFT

POL00423684

Cyber Security Update

4

Author: Tony Jowett Sponsor: Shikha Hornsey Meeting date: 25 November 2019

Executive Summary

Context

This paper describes how we are increasing the maturity of our cyber defences, what are the early results of the DLP pilot and what we are doing to minimise the risk of the insider threat.

Questions this paper addresses

- What progress have we made in achieving our maturity targets?
- What are the early results from our DLP pilot?
- How are we reducing the risk associated with the insider threat?

Conclusion

1. After having closed all high-level recommendations, we continue to deliver on the highest priority actions on the detailed recommendations. Detailed progress is included in this paper and a plan is included in the Appendix. We continue to be on track to reach our target maturity by March 2020 whilst recognising that in subsequent years we will need to continue to deliver security improvements in response to changing business needs and threats.
2. The DLP pilot continues to make good progress with some early statistics relating to our admin estate. The DLP scanning toolkit identified a data breach in Post Office Insurance which has subsequently been acted on.
3. Insider Threat risks are being reduced by the development of security tooling in DLP, the Security Operations Centre (SOC) and threat intelligence. In addition, a coherent programme of activity over and above the tooling is now required to consciously track and mitigate these risks.

Input Sought

The ARC is requested to note the progress made and provide feedback on the report.

POL00423684

Report

What progress have we made in achieving our maturity targets?

1. Having completed all the high-level recommendations from the Deloitte report we continue to focus on reducing the gap between current and target maturity under the IT Security Transformation Programme (ITSTP).

2. We have included a Gantt chart showing the plan for the ITSTP in the Appendix A. We are aiming to hit target maturity by March 2020. In subsequent years we will need a rolling programme of security improvements to keep Post Office safe in response to developments in the business, the changing nature of the threats faced and the opportunities arising from developments in defensive technology.

3. The status of the remainder of the programme is as follows:

Area	Milestone Completion			Target Completion Date	Update
	Target	Previous	Current		
Deloitte Cyber Review Actions	65%	52%	59%	March 2020	Continue as planned. When larger dependant projects complete (i.e. DLP) significant volumes of actions will conclude in a single update.
Deloitte Information Protection Review actions	65%	45%	51%	March 2020	Continue as planned, as above
RSA Archer implementation	40%	31%	43%	Feb 2020	Recovery of some initial delays due to "BluePrint" have been achieved, designs complete and POCs are being developed presently.
DLP	15%	13%	16%	Feb 2020	Discovery in full flight, action-able data already being used by DPO and PCI compliance. Policy design progressing well.
SOC Maturity	Treated as ongoing continual improvement to BAU. Widening coverage of SOC through acquisition of more logs including Payzone and Post Office Insurance.				

4. Based on this assessment the gap between the current and target maturity levels of Post Office has been reduced by 54% (last report was 44%) since the start of the programme in March 2019.

5. Whilst the progress to date has been good there is still much to do to achieve our targets and progress is dependent on other areas of post office being able to deliver their parts.

POL00423684

6. We are conducting an internal-audit led review of our maturity target completion. We are scheduling a full Deloitte-led maturity retest for April 2020.

7. In addition to this work we are now beginning a refresh of our Cyber Strategy for 2020 onwards taking input from the business, new threats and technologies.

What are the early results from our Data Loss Prevention (DLP) pilot?

What is DLP?

8. DLP refers to a range of technologies and controls aimed at preventing the loss of sensitive/confidential data from the organisation either by accidental or malicious means. As Post Office is one of the few really trusted brands on the UK high street then DLP is key to keeping those trust levels high by securing the data we hold.

9. DLP helps protect Post Office data and intellectual property but also helps us to be compliant with the UK Data Protection Act (2018) which embodies the EU General Data Privacy Regulation (GDPR). The UK has always had such legislation, but the fines associated with data breaches have increased in this iteration of the act to a maximum of 4% of global turnover.

10. The UK Information Commissioner's Office are responsible for running investigations into data breaches with focus on personal and sensitive personal data.

11. Without DLP we have no way of controlling what data is leaving our organisation. Additionally, when we experience a data breach then DLP technology will help us to rapidly contain it, locate the source and fulfil our reporting obligations to the ICO thereby reducing the risk of a major fine.

12. There is a balance to be achieved with DLP where non-sensitive data can be freely exchanged whilst the activities around sensitive items are restricted appropriately. This requires precision in identifying data and controls to stop sharing data. Therefore, we are implementing DLP in two phases:

    a. Learning mode where the tools analyse the movement of data in the organisation

    b. Control mode where, based on the above analysis we implement controls to appropriately control sensitive data leaving the organisation

What have we done so far?

13. After a procurement exercise we selected the Microsoft suite of tools based on functionality, ease of implementation and price. We have run a pilot on these tools which has been extremely helpful. For this pilot initial Post Office DLP rules have been developed and are now active alongside the out-of-the-box threat rules from Microsoft. The resulting output has created a considerable degree of threat intelligence data for the ASOC (Advanced Security Operations Centre), Data protection office and PCI compliance.

14. The DPO and PCI compliance teams are feeding critical insights and lessons learnt back to the DLP analysts to maintain a continuous fine-tuning process. Initial communications to the user population are soon to be distributed with further communications planned as progress develops.

POL00423684

15. Statistics from early scans

- 18.8 Million files scanned across the Post Office 365 environment
- 2800+ Web Applications are in use with some including data uploads and downloads. Volumes of users by application have been gathered. Applications that clearly are in breach of the Acceptable User Policy have been blocked e.g., Dropbox, Slack etc.
- Inbuilt DLP policies exist to cover items such as;
    - External and unusual sharing
    - Mass file deletion,
    - Unusual travel activities,
    - Unusual downloads.
- Post Office-specific DLP policies have been developed in the tools to look for the following on outbound emails;
    - PCI data
    - Medical Records
    - PII
    - General Financial data

Post Office Insurance data breach investigation resulting from DLP pilot

16. A member of staff undertaking an MBA incorrectly used data supplied to us by third party claims managers. This was detected by DLP. He had removed the names from this data and has then shared it by email with fellow MBA students with a view to using this data as part of an MBA project.

17. The data utilised contains policy numbers, age, post codes and some information on the type of claim made including details of where a claim was related to a death or a medical condition. It does not contain bank account or credit card details. It is estimated that 19,300 records are impacted. The data covers claims made from 2017-2019.

18. There is no suggestion that the use of data was in anyway malicious. However, given the use of post codes, policy numbers and some medical data it does constitute a data breach given the data is individually identifiable and has been passed external to Post Office without adequate controls, and for a purpose which customers would not have provided clear consent.

19. The member of staff concerned was suspended whilst further investigation work was completed. We have contacted our insurance partners to make them aware of the issue, and the recipients of the data have deleted this data and confirmed deletion.

20. The member of staff involved had completed mandatory data security training. A reminder of our approach to data security has been issued to all staff.

21. This issue has been reported to the ICO and FCA.

22. This breach was only discovered as a result of implementing the DLP scanning.

What's next

23. The next stages of the project will commence testing of the AIP (Azure Information Protection) software which manages the data classification process. The test of AIP will be to a limited audience with DPO and PCI compliance being actively involved.

POL00423684

How are we reducing the risk associated with the insider threat?

What is Insider Threat?

24. Insider threat is when a current or ex-colleague, contractor or business partner, who has (or had) authorised access to Post Office systems, information assets or premises, uses that access to compromise the confidentiality, integrity or availability of Post Office's information assets. This can be with or without malicious intent.

25. Insider threats can be accidental and non-malicious where colleagues seek to circumvent process and controls to short-cut activities to get something done. They can also be malicious such as a colleague obtaining customer details for a specific product, and then selling those details to a competitor. In both cases the results of these actions can be serious and escalate to have impacts that are fraudulent, regulatory or criminal. Examples of recent insider threat activities outside Post Office and their impacts are included in Appendix B.

26. Insider threats tend to peak when an organisation goes through significant changes in leadership, structure, purpose and size. Post Office is currently undergoing such significant changes.

27. The threats created by insiders are hidden in plain sight as the perpetrators do not need to "break in" to gain access to data and crown jewels. Also, their illicit activities are harder to detect than an external attacker.

28. Although technology can play an important role in identifying potential insider threats, it is not just an IT issue. It takes an enterprise-wide approach covering multiple disciplines, to plan for, prevent, detect, respond to and recover from insider threats.

What are the types of insider threat and what is our proposed approach?

29. There are two main types:

    a. **Direct Threat** - Abnormal activities that deviate from the normal pattern that an individual or group of individuals follow. Examples include downloading large volumes of data to external drives, accessing sensitive information that bears no direct relevance to normal job duties or emailing confidential data to a personal account.

    b. **Indirect Threat** - Is usually shown by patterns of human behaviour that require analysis to reveal suspicious motives. Examples include sudden overuse of negative emotive words in electronic communications, expressing desire to resign over social media, or demonstrating ties to high-risk personnel or outside parties.

30. We are initially focusing on Direct Threats as experience shows that technology to track Indirect Threats is still in its infancy, and the actual success rate is less than 1% of discovering a colleague who intends to do damage before they attempt to do so.

What do we have in place currently to help with insider threat?

31. We have focused on putting in place the pre-requisite detection capability for an insider threat programme, namely:

    a. **SOC** maturity expansion and coverage enhancement

    b. **Data Loss Prevention** technology

    c. **Dark Web Monitoring** (Recorded Futures) to identify on-line malicious intent regarding Post Office

POL00423684

What are the next steps?

32. For the remainder of this calendar year

    a. Develop the foundations and scope for the programme

        i. Initiate a programme to deliver an increase in maturity for insider threat

        ii. Initiate cross-programme governance covering IT, Cyber, HR, union reps and third parties

        iii. Determine appropriate Measures and KRIs and reporting mechanisms frequencies

        iv. Review of risks and mitigations appropriate to POL

        v. Complete planning for remainder of project with input from external sources and in-house testing

33. In the first quarter of 2020

    a. Implement a base level culture and awareness programme applicable to all insider populations

    b. Identification of "privileged" insider populations within POL and agree appropriate measures for training, awareness and checking/monitoring

    c. Increase the frequency of messaging from the most senior leadership regarding positive security behaviours based on specific topics with emphasis also on consequences of bad behaviours

    d. Develop guidance for line management to help spot insider issues

    e. Review our third parties and their approach to managing insider threat

    f. Baseline metrics and KRIs

34. In the second quarter of 2020

    a. Extend the Post Office Insider Threat activity to our third parties and their third parties where appropriate

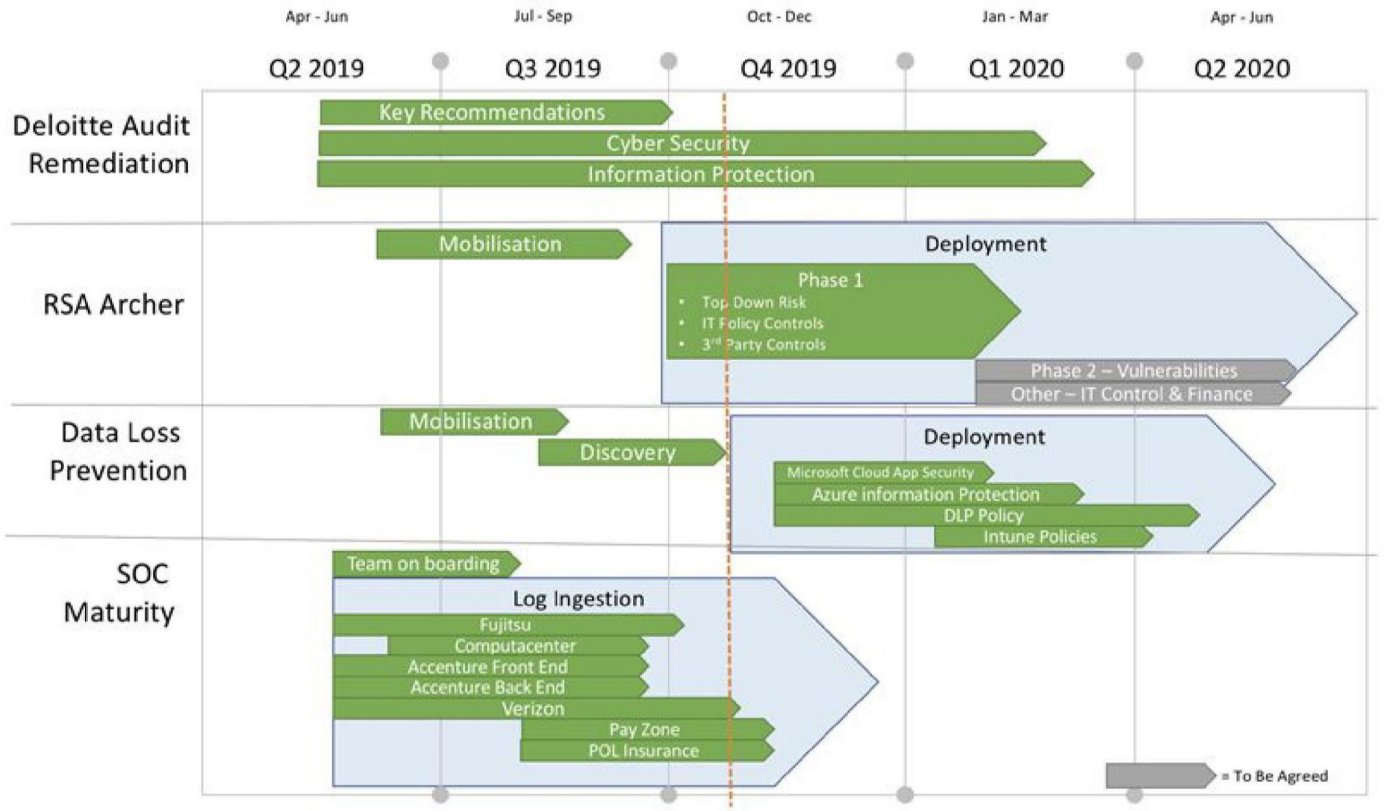
    b. Implement random spot checks on account usage; identification, maintenance and monitoring of a list of high-risk roles; targeted education and awareness campaigns; and, use of disciplinary action for behaviour that is inconsistent with POL policy and values

    c. Increase the scope of the logging and monitoring of the various systems and applications that are being leveraged across the third-party suppliers. This will likely to be a resource intensive and expensive proposition

    d. Publish reporting and metrics

POL00423684

Appendix A ITSTP 2019/20 Plan



POL00423684

Appendix B What has happened to other organisations as a result of insider threats

UK companies affected recently by malicious insiders:

- **Capital One** - A hacker gained access to 100 million Capital One credit card applications and accounts
- **Morrisons** – employee extracted payroll data and published on the dark-web
- **Ofcom** - employee downloaded 6 years' worth of third-party data for malicious use
- **69%** of organisations **have experienced an attempted** or **realised data theft** by **insiders** (Source: Accenture 2016)
- **£1.32** million per organisation to resolve a breach caused by an insider (Source: Info Security Group)
- **50 days** to recover from a cyber event (Source: Accenture)

Other Cyber threats that can be influenced by insiders, either maliciously or inadvertently

- **Ransomware** attacks are **growing by 350% annually**. (Source: Cisco)
- **1 in 13** web requests lead to malware infection attempts (Source: Symantec)
- **71%** of attacks are generated by **phishing emails** (Source: Accenture)
- **31%** of organisations have **experienced cyber attacks**. (Source: Cisco)
- **147.9 million** consumers affected by the Equifax Breach (Source: Equifax 2017)
- **400,000 machines in 150 countries were infected** by '**Wannacry**', costing @**$4 billion**. (Source: Malware Tech Blog 2017)

POL00423684

Contract Management Framework Update

Author: Sherrill Taggart/Ben Foat Sponsor: Ben Foat Meeting date: 25 November 2019

Executive Summary

Context

Although controls have been introduced over the last few years (e.g. central repository for contracts, CAF process etc.), poor contract management remains a risk and prevents Post Office from capitalising on revenue generating opportunities, foments inefficiencies, impedes communication and collaboration, and can trigger risk and other compliance issues.

There are inconsistent levels of expertise across the business of how to manage contracts, and specifically, the contractual obligations imposed on each party and their impact to other areas within the business. Examples of poor contract management include:

- Contracts having expired without new written contracts being put in place;
- Services being provided or received from third parties without a contract in place;
- Key contractual obligations not understood or monitored leading to breach of contract;
- Wasted spend and resources arising from poor planning and/or due to limited contract management tools;
- Operational inefficiencies e.g. unable to identify or locate contracts, deviations from standards are not tracked, rights and benefits under the contract not being received.

The successful implementation and operation of the Contract Management Framework (the Framework) is dependent on a cultural change whereby contract management is recognised as a core skill at Post Office with those responsible for the management of third party relationships being provided with appropriate tools and infrastructure but also held to account for incidents of non-compliance.

Questions addressed in this report

1. Why do we need to manage this risk?
2. What is the objective of the proposed Framework and why is this important to the Post Office?
3. What is the proposed approach on how contracts should be managed and what are the possible HR and budget implications for this structure?

POL00423684

4. What are the further budget considerations for the roll out of the Framework and the continued development of Source 2 Settle?
5. What do we need to do next to progress the finalisation, adoption and implementation of the Framework?

Conclusion

1. Contract management not only enables the parties to work together to achieve the commercial objectives but it also deals with any short comings, contract changes, extensions and renewals and finally exit and transition. The key risks or consequences arising from poor or no contract management include:

   - Failure of the contract to fulfil its commercial objectives;
   - Failure to protect the rights of the parties;
   - Failure to ensure performance and compliance when circumstances change;
   - Reputational risk;
   - Fraud or error; and
   - Contractual disputes and third party damages action.

   In order to manage the above risks, a Contract Management Framework has been developed, the purpose of which is to provide a clear and standardised management and governance structure - the adoption of which enables the effective management of contracts and Post Office's suppliers and clients. The Report sets out a summary of the key elements of the Framework.

2. The objective of the Framework is to set out the approach, roles and responsibilities, internal controls, process, and operational standards which allow the most efficient and effective management of Post Office Group contracts and partners. By ensuring effective contract and relationship management, Post Office decreases its exposure to operational, commercial and financial risk.

3. The Framework envisages a cost efficient decentralised model which introduces clear accountability to those managing the contracts and intends to utilise technology (through Source to Settle (S2S)) to provide a basic centralised view over contract management. An alternative option would be to establish a centralised or hybrid contract management team but at this stage this is not recommended due to costs and the disadvantages of separating relationship and contract management. The recommendation at this moment, pending the Purpose, Strategy and Growth Review ("PSG Review") is to formalise the decentralized model given it is more cost efficient and less disruptive but to review the position after the PSG/Org Design review.

POL00423684

The proposed approach to implementing the Framework will be to onboard the top 50 material contracts based on financial and strategic value together with a sample of supplier, HR, IT software and network agency contracts. These should then be managed in accordance with the principles and guidelines of the Framework. The Annexure to the Report provides a summary of the Framework and lists the material contracts which will be ratified with the business to identify the top 50 material contracts as mentioned.

4. The formalisation of the roles of the Contract Owner and Contract Manager are key to the operation and success of the Framework. In order to be able to identify individuals and assign roles, responsibilities and accountabilities, there will need to be upskilling or creating capacity for appointed Contract Owners and Contract Managers to own and manage contracts with accountabilities and responsibilities around contract management recognised and reflected in Job Descriptions and annual objectives. Incidents of non-compliance should be monitored and ultimately reported to ARC to ensure that contract management performance is within risk appetite.

5. A necessary enabler of the Framework will be the WEB3 system (S2S) which is the current web-based eProcurement platform which Contract Managers (with support from the Procurement and Legal Team) will need to use to manage their contracts. Ongoing investment will be required for this platform to ensure the continued effectiveness of the Framework and to use the data in the contracts to the Post Office's commercial advantage. Further possible funding requirements are as follows:

   (i) Source 2 Settle (S2S):
   - User licenses for Contract Managers;
   - Transfer of contracts from Bravo and input into S2S; and
   - Installing all contract templates.

   (ii) Training materials which will be provided by the LCG Function.
   (iii) Resourcing of Contract Management Teams (subject to above).

6. Next steps for the roll out and implementation of the Framework include:

   (i) Approval of the Contract Management Framework at the November ARC meeting.
   (ii) Developing an implementation plan including finalising budget/funding requirements and timeline.
   (iii) Presenting business case for funding for approval to Project Review Board.
   (iv) Go live of Source 2 Settle.
   (v) Initiating the implementation plan.
   (vi) LCG Academy – Contract Management Training.

POL00423684

7. The Framework is an evolving document and may need to be amended following the outcome of the PSG Review. While some input has been received from key stakeholders in the businesses and functions and incorporated in the Framework (which is available in full in the Reading Room or in summarised form at Annex 1), discussions are ongoing with the key stakeholders to obtain their comments. Further, this paper has been presented and discussed at both RCC and GE and has full executive sponsorship.

Input Sought

The Committee is asked to:

1. Note the update on the progress of the development and implementation of the Framework.

2. Discuss and approve in principle a decentralised contract management model and approach.

3. Note the potential budget requirements and dependencies for the implementation and maintenance of the Framework and Source 2 Settle.

Input Received/Sought

1. Barbara Brannon (Procurement)
2. Shihka Hornsey (IT) / Dione Harvey (IT)
3. Lisa Cherry / Emma-Rose Bonner (HR)
4. Mark Siviter (Mails) / Martin Kearsley (Banking) / Andrew Goddard (Payments) / Debbie Smith (Retail)
5. Julie Thomas. Tim Perkins, Jason Mumby and Nick Beal (Network Agency contracts)
6. Chrysanthy Pispinis (Financial Services)

POL00423684

The Report

The Proposal

To develop a Contract Management Framework (the "Framework") for the Post Office Group which provides a clear and standardised management and governance structure – the adoption of which enables the effective management of contracts and Post Office's suppliers and clients.

The Objective

The Framework sets out a clear decentralised model of accountabilities and responsibilities at the various stages of the contract management lifecycle from the establishment of the business case through the contract administration and relationship management, the review of contract performance and finally contract close-out and transition.

The Framework sets out the roles and responsibilities, internal controls, process, procedures and standards that are necessary for the Post Office to be able to efficiently and effectively manage its contracts across the Group. Effective contract management is important as it enables Post Office to:

- Ensure it has the right people with the right capabilities in the contract management roles;
- Have the visibility required for contract management to operate as an effective and multi-disciplinary function (e.g. involving Finance, Procurement, Legal, Commercial, Operations etc.);
- On-board appropriate and adequate suppliers and clients, in accordance with prescribed processes designed to protect Post Office;
- Enter only into contracts which include acceptable and manageable risks;
- Leverage its rights under the contract and manage the relationship and performance of its suppliers and clients effectivity;
- Bring the best outcomes to customers by evolving and developing new solutions with its partners;
- Ensure ongoing contract compliance and performance, reducing contractual and commercial risks through robust contract management practices;
- Effectively deliver contracts at or under the agreed costs and rates and identify savings and revenue opportunities throughout the contract management process; and
- Efficiently exit and on-board replacement partners to continue providing its products and services with a minimum impact on customers.

POL00423684

Scope of the Framework

Contract Life Cycle

The Framework is intended to provide an overarching framework the activities associated with the contract management lifecycle which is set out below:

PHASE	STAGE	TASK
PHASE 1	Transition/Setting up	Contract award – execution – service delivery / commencement
		Classify contract based on value and risk
		Confirm Contract Management roles
		Finalise Contract Management plan
		Set-up information management structure
PHASE 2	Contract Management	Manage performance
		Contract Administration
		Risk Management
		Manage contract extensions / renewal / variation
PHASE 3	Close-out	Final performance review
		Lessons learned
		Contract close-out/transition

Types of Contracts

The following are the main contracts/agreements used at the Post Office:

- Supplier Contracts
- Client Contracts
- Network/Agency Contracts
- Banking Framework Contracts
- IT Contracts
- Software Licenses
- Employment contracts
- Data Sharing Agreements
- Property
- Non-disclosure Agreements

POL00423684

Roles & Responsibilities

There are two essential roles for managing contracts effectively. Each role draws on a range of skill sets.

Roles of Contract Management	
Contract Owner (CO)	• Person accountable for the budget/cost centre that funds contract and the performance of the contract • Employee with delegation to approve contract payments and variations • Appoint contract management roles • Recommended to be a senior employee who is impacted by the contract outcomes
Contract Manager (CM)	• Day-to-management of contract lifecycle from tender to exit • single point of contact for suppliers and clients on all contract matters • Monitor contract performance and compliance • Recommend to be a representative within the business unit with the relevant skills • Perform administrative activities over the contract management lifecycle (e.g. information management, cost control, etc.)

Contract Managers play a critical role for the Post Office as they direct and oversee contracts throughout their lifecycle. Serving as the liaison between companies, employees, customers, vendors, and independent contractors means contract managers serve as the main facilitators for negotiations, recommendations, record keeping, monitoring, change management and more.

The Contract Manager must have:

- appropriate skills (both specific contract management skills and more general commercial awareness and expertise) with access to the relevant training and development;
- accurate job descriptions. Roles must be positioned at an appropriate level and compensation and there should be a career path for contract management staff;
- clear objectives and reporting lines. Their performance will be managed through reviews and appraisals;
- appropriate delegated authority to manage the contract effectively;
- detailed knowledge of the contracts they manage and other related issues, such as service level agreements and ongoing supplier performance;
- knowledge of the organisational governance, processes, risk structures and organisational risk appetite; and

POL00423684

- clear objectives to manage their contracts including compliance with its terms and conditions.

When deciding on the on the appropriate Contract Manager it is important to take into consideration the following:

- Does the contract need to be managed by someone with specialist skills and experience i.e. resources should be tailored to the materiality, risks and opportunities provided by the contract?
- Do the individuals have the required experience, knowledge and authority for the role given the contract classification and risk profile?
- Do they have enough time to carry out the role?
- Can the person carry out multiple roles?
- Are they willing to take accountability for the role?
- Do they have any private interests or relationships that may give rise to claims of conflicts of interest (perceived or actual)?
- Identify how the contract fits into the wider portfolio of contracts; and understand staffing requirements across material and strategically important contracts;

Contract management objectives should be included into Personal Development Plans for Contract Owners and Contract Managers. Objectives will need to be clearly set out and agreed with performance against the objectives being managed through reviews and appraisals.

Proposed Approach to Implementation

Implementation steps will include:

- Target top 50 material contracts based on value together with samples of supplier, HR, IT software and network agency contracts.
- Assign Contract Owners and Contract Managers to top 50 contracts.
- Ensure all Contract Managers are trained up on Source to Settle.
- Obtain confirmation all contracts are in place and loaded on Source to Settle.
- Contract Obligation spreadsheet and CAFs are known and understood.
- Alert set for all key contract dates.

How will success be measured?

The Framework will benefit from having clear KPIs in place to provide evidence of the level of achievement of the aim to optimise processes and to deliver favourable outcomes. Requisite KPIs such as contracting cycle length, consistent quality, schedule adherence and cost effectiveness will need to reflect desired outcomes:

- Minimal time to signature;
- Minimal changes to agreed contractual language;
- Minimal avoidable business risk;
- Best possible value for contract agreements and contract renewals;

POL00423684

- Adherence to contract management processes and optimisation of contract management processes; and
- Maximizing compliance.

Performance targets should be regularly reviewed to ensure the KPIs remain relevant and meaningful.

What do we need to do next to progress?

1. Approval of the Contract Management Framework at the November ARC meeting
2. Obtain agreement and approval from ARC on the proposed approach for the Contract Management Team.
3. Develop an implementation plan including finalising budget/funding requirements and timeline.
4. Present the business case for funding for approval to Project Review Board.
5. Go live of Source 2 Settle.
6. Initiate implementation plan.
7. Report back to ARC in March 2020.

POL00423684

Annex 1: Framework Overview

Planning: Vendor and Business Opportunity	**On Boarding:** Suppliers and Clients Due Diligence	**Contract Formation:** Creation, Negotiation, Execution, Obligations Tracking and Exit	**Acceptance of Risk and Contract Execution**	**Contract Management**	**Contract Close Out and Transition**
• Alignment with business strategy. • Resourcing requirements. • Budgetary requirements to meet contractual commitments. • Other requirements e.g. IT, systems and processes, 3rd parties etc. • Is it in the best interests of the company?	• Vendor screening – suitability, credibility and ability / capacity to deliver. • Ongoing monitoring of performance (SLAs, KPIS etc) and financial screening (Dunn & Broadstreet) - particularly for IT Suppliers and Insurers. • Pricing reviews. • Procurement process.	• Contract Management Team roles and responsibilities. • Types of contracts. • WEB3 – Digital Contract Management Toll. • Responsibility for commercial terms, including services schedules, pricing and SLAs.	Assessment and Acceptance of Risk: • Risk Appetite. • Legal Risk Notes. • Exceptions Approvals. Contract Approval Process: • eContract Approval Forms. • Authority to Sign. • Execution of contracts. • Storage of contracts. • Retrieval of contracts	• Contract Management Team. • Plan, resource and management. • Contractual terms. • Risk management. • Developing Internal and external relationships. • Wax obligation mapping. • Feedback and Communication. • Payment and budgets. • Performance reviews. • Managing wider market issues. • Handling of contract amendments, variations and extensions. • Managing complaints and disputes. • Contract management tools	• Managing contract close out. • Re-procurement. • Final performance review. • Finalising contract close out, including any transition.

Roles & Responsibilities

Roles of Contract Management		
Contract Owner (CO)	Recommended to be a senior employee who is impacted by the contract outcomes. • Person accountable for the budget/cost centre that funds the contract and the performance of the contract. • Employee with delegation to approve contract payments and variations. • Appoint contract management roles.	
Contract Manager (CM)	The Contract Manager play a critical role for the Post Office as they direct and oversee contracts throughout their lifecycle. Serving as the liaison between companies, employees, customers, vendors, and independent contractors means contract managers serve as the main facilitators for negotiations, recommendations, record keeping, monitoring, change management, and more.	The Contract Manager must have: • Appropriate skills (both specific contract management skills and more general commercial awareness and expertise) with access to the relevant training and development. • Accurate job descriptions, roles are positioned at an appropriate level and compensation and there is a career path for contract management staff.

Post Office Limited - Audit Risk & Compliance Committee-25/11/19

POL00423684

	• Day-to-management of contract lifecycle from tender to exit. • Single point of contact for suppliers and clients on all contract matters. • Monitor contract performance and compliance. • Recommend to be a representative within the business unit with the relevant skills. • Perform administrative activities over the contract management lifecycle (e.g. information management, cost control, etc.).	• Clear objectives and reporting lines and their performance is managed through reviews and appraisals. • Appropriate delegated authority to manage the contract effectively. • Detailed knowledge of the contracts they manage and other related issues, such as service level agreements and ongoing supplier performance. • Knowledge of the organisational governance, processes, risk structures and organisational risk appetite. • Clear objectives to manage their contracts including compliance with its terms and conditions.
Supporting Roles	• **Finance Approver**: A person who ensures that any financial exposure under a contract is understood and can be fulfilled by Post Office and approves such exposure, i.e. the relevant Finance Director for the area in which the contract originates. • **Procurement:** A procurement category manager who supports the business colleagues with sourcing the right supplier, negotiating the best deal, assisting with management of contract changes, assisting with market intelligence and management of suppliers. • **Legal, Compliance and Governance Colleagues**: Colleagues who provide expertise for areas where the contractual, legal or regulatory exposure is greater. They will also provide frameworks and guidance on appropriate controls (including templates, FAQs and training) to Contract Owners and Contract Managers. They will also support the negotiation of these instruments as well as any disputes which may arise.	

Assessment and Acceptance of Risk

Contractual and operational risks	Post Office has specified its risk appetite in respect of contractual and operational risks in existing and new relationships. Therefore, all employees at Post Office must act within those defined the levels in order to avoid unauthorised exposure.
Legal and regulatory risk	Post Office has set out the following levels: • 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 Post Office staff.
Legal Risk Notes: When dealing with contracts every stakeholder should bear in mind the acceptable levels of risk, to ensure that any risks accepted are not greater than they should be. One of the tools that the Legal Team will equip the Contract Manager and Contract Owner with a Legal Risk Note which sets out the contractual risks and mitigants. Contract Managers should ensure that the mitigants remain enforce/effective during the life of the contract. Exceptions: 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. Therefore, if Post Office is going outside of the accepted approval processes, an exception report (using the Risk Exception template) needs to be prepared and approved.	

Post Office Limited - Audit Risk & Compliance Committee-25/11/19

POL00423684

Control Standards

A minimum control standard is an activity which must be in place in order to manage exposure so that it remains within the defined acceptable parameters for Post Office. The table below sets out the relationships between identified risk and the required minimum control standards in consideration of the stated risk appetite.

Applicable Area	Description of	Minimum Control Standards	Who is responsible	When
Contract Award	Not procuring contracts in accordance with Public Contract Regulations means, that for POL, they are being awarded non-compliantly	All non-compliant contracts must be reported as a risk up to the Procurement Director who in turn reports up to the RCC.	Procurement Director	Always
		Engagement with Procurement from an early stage when procuring goods and services	Contract Managers	Always
		Demand Management Programme guidance	Legal	Should be used when appropriate, updated by Legal when necessary
		Ongoing training to the Procurement team and wider business	Legal	TBC
Contract Execution - Unauthorised signatories signing contractual documents, including electronically	The company is entered into a legally binding contract or obligation without internal approvals and independent oversight.	Only the Company Secretariat can distribute contractual documents for signature (including via e-signature software). • Process: All contract signatures must be facilitated by the Secretariat and supported by a relevant internal authority evidenced in a contract approval form "eCAF" unless a written exception has been agreed by the Company Secretary (e.g. Employment Contracts facilitated by HR or Franchise Agreements facilitated by the Retail). • Assurance: The submission of an eCAF in accordance with the contract approval process will satisfy the delegated authorities approved by the Board and maintained by the Company Secretary. • Oversight: Only authorised signatories who are not also signatories to the relevant eCAF (to prevent a conflict of interest) will be requested to sign contracts unless a written exception has been agreed by the Company Secretary. • The list of authorised signatories is maintained by the Company Secretary following Board approval.	Company Secretariat All Employees	Always

POL00423684

		Training: Guidance on the company intranet page(s) is updated regularly to provide the business with accurate information on the contract approval and execution processes, including the authorised signatories.	Company Secretariat	TBC
		Awareness: Twice yearly communications will be sent to all colleagues to remind them about governance processes and procedures, including authorised signatories.	TBC	Bi-annual comms plan
Contract Management	A lack of understanding of how to manage contracts efficiently, knowledge of contractual obligations on each party, impact to other areas within the business and basic contract law gives rise to risk of not meeting contractual obligations, being unable to pursue action in event of breach or last minute resource implications when contracts are suddenly about to expire or need to be renewed.	Contract obligation mapping on WAX will allow mapping of key deliverables or actions that each party needs to undertake to comply with the contract	Contract Managers	Always
		Central repository of contracts to ensure contracts and appropriate additional information is accessible	Procurement/Contract Managers	Always
		Legal training to the business to improve their understanding of the contractual obligations and impacts of contracts on other areas within the business	Legal	
		Developed house positions with playbooks that set out a range of acceptable negotiated positions for the following contract types: supplier contracts, bill payment contracts, agency network contracts and employment contracts	Legal	To be used when appropriate, reviewed by Legal on an ad hoc basis

POL00423684

Annex 2: Material Contracts to be ratified with the Business

Area	Contract Name	Other Party
CFO	Audit of Notes Circulation Scheme, MDA, DVLA BIS loan	Ernst & Young
CFO: Procurement	Source to Settle - Sourcing and Contract Management Portal	Wax Digital
CFO: Supply Chain	Supply of fuel for commercial vehicles to 4 x Supply Chain depots with own fuel bunker facilities	Certas Energy
CFO: Supply Chain	Provision of Goods and Services relating to cash cases and cash valuables in transit	Spinnaker International Limited
CFO: Supply Chain	POL Vehicles Framework	Torton Bodies Limited
CFO: Supply Chain	Note Circulation Scheme	The Bank of England
CIO	Horizon IT hardware, application, data centre and network services	Fujitsu Services Limited
CIO	Network IT Tower contract	Verizon
CIO	Safe Haven.	CSC
CIO	Common Digital Platform Agreement	Accenture
CIO	Back Office IT Tower contract	Accenture
CIO	End User computing (provision of equipment & support/maintenance)	Computacenter
CIO	Licenses for Salesforce CRM Application used by frontline and back office support to FS and MS including CRM and Website lead capture	Salesforce
CIO	Agreement relating to Service Integrator and Service Desk Services	Atos IT Services UK Limited
CTO	Post Office Transformation Agreements	Co-Operative Group Food Limited
CTO	McKinsey & Company Consultancy Services	McKinsey & Company Inc UK
Finance and Ops	Supply of fuel for commercial vehicles for withdrawal at garage forecourts nationally and also to 1 x Supply Chain depot with own fuel bunker facilities	Watson petroleum (Hall fuels)
Finance and Ops	Grapevine	Kings Security Services
FS	Card Payments	World Pay
FS	Facilities Agreement	Royal Bank of Scotland
FS	Research and Insights	Quadrangle
FS	Provision of Communication - Creative and Delivery Services.	DLKW Lowe
FS	Print Management	HH Associates Limited
FS: Brand	Creative Agency	Ogilvy & Mather Group (Holdings) Ltd
FS: Identity	Verify ID Checking	Digitentity
FS: Identity	Verify ID Checking	DWP (Cabinet Office)
FS: Identity	Driving Licences	DVLA
FS: Identity	Biometric Enrolment - Overseas Applicants	UKIV
FS: Identity	Passport Check & Send	HMPO
FS: Identity	Biometric Enrolment - Domestic Applicants	UKIV
FS: Identity	IT support for Application, Enrolment and Identity Services	Gemalto
FS: Marketing	Data Analysis, Direct Mail, Email & SMS	RAPP
FS: Post Office Money	Joint Venture Agreement	Post Office and 1. First Rate Enterprises Limited (BOI) 2. FRTS 1 Limited (FRES)
FS: Post Office Money	Agreement for the Provision of Money Transmission Services	MoneyGram Payment Systems, Inc
FS: Post Office Money	Financial Services Joint Venture Agreement	Bank of Ireland
FS: Post Office Money	Travel Money Card	FRES and FIS
FS: Post Office Money	International money transfer & Online	FRES (First Rate)
FS: Telecoms	Core Telecommunications Network connecting Post Office Crown and Admin sites	Verizon
FS: Telecoms	Agreement for the Provision of Post Office Homephone and Broadband Services	Fujitsu Services Limited
FS: Telecoms	Contract relating to provision of Services relating to payment of billing services	BT Telecommunications plc
HR	MySAP Software License & Maintenance Agreement	SAP UK Limited
HR	Interims and Contractors	Sopra Steria
HR	An on-line advisory service	Adviser plus
HR	Security Vetting	Experian
HR	Long Term Incentive Plan Awards	Post Office Limited
HR:	Provision of occupational health and wellbeing services to Post Office	Atos IT Services UK
HR: Culture	Staff Engagement Survey	Aon Hewitt Ltd
HR: ER	Collective Engagement Framework	Unite
HR: ER	Collective Engagement and Industrial Relations Framework	CWU
HR: Pensions	Pension provider - Money4Life Service Agreement	Zurich
HR: Shared Services	Pay data	Hay Group
POL	Distribution Agreement	Post Office Management Services
POL	Master Services Agreement POL and POMS	Post Office Management Services
POL	Government Funding- Provision of network	BEIS
POMS	Car, Van and Home Insurance	Budget Insurance Services Ltd
POMS	Travel Insurance	Collinson Insurance Services Ltd
POMS	Technology Services	Hexaware Master Services Agreement & MI
POMS	Life Insurance	Royal London Life Contract
POMS	Duck Creek Policy	Accenture
POMS	POL's Outsourced Contact Centre (Travel, General Insurance and other Products) (POMS)	Telecom Services Centres Limited t/a Webhelp
Retail	Agency Branch Network	Postmaster/Main/Local
Retail	Rod & Game	Environment Agency
Retail	Collaboration Agreement	POL, WHSmith High Street Limited and WHSmith Travel Holdings Limited

POL00423684

Area	Contract Name	Other Party
Retail	Framework Concession Agreement	POL, WHSmith High Street Limited and WHSmith Retail Holdings Limited
Retail	Crown Transformation - Self Service Kiosks (SSK's)	NCR Ltd
Retail	Gift and Savings Cards	The Gift Voucher Shop
Retail	One Stop Servicest	Lord Mayor & Citizens of Westminster/ Hammersmith & Fulham Borough Council
Retail	Grant Agreement- Support NT	NFSP
Retail	Master Franchise Agreement (MFA)	Post Office and WHSmith
Retail	Standard Individual Branch Mains Agreement as set out in Schedule 8 of the MFA (Mains Agreement 2016)	POL and WHSmith High Street Limited (various dates)
Retail	The National Lottery Retailer Agreement	Camelot UK Lotteries Limited
Retail	Estate Management & Asset Valuation Services	BNP Paribas
Retail: Banking	POCA	Electronic Data Systems
Retail: Banking	POCA	DWP
Retail: Banking	ATM Charges Agreement	J.P Morgan
Retail: Banking	Cheque Processing & Clearing	Barclays
Retail: Banking	Link network Services Agreement	Vocalink Limited
Retail: Banking	ATM agreement	Bank of Ireland
Retail: Banking	Banking Framework	Various
Retail: Bill Payments	Merchant Acquiring Service Agreement	Global Payments UK
Retail: Bill Payments	Paystation Agreement	Ingenico
Retail: Bill Payments	Reseller	Various
Retail: Bill Payments	Payout Agreement	Various
Retail: Bill Payments	Direct Bill Payment Agreement	Various
Retail: Bill Payments	Supply of Half Hourly Electricity	EDF Energy Customers plc
Retail: Mails	Mailwork Agreement	Royal Mail
Retail: Mails	Swindon Warehousing Services Agreement	Royal Mail
Retail: Mails	Mails Distribution Agreement	Royal Mail
Retail: Operations	Hard maintenance services	CBRE [acquired Norland]
Retail: Operations	Provision of Goods and Services relating to Safes and Secure Cash Storage	Insafe International Limited
TBC	Market Research and Insights Framework	KPMG Nunwood Consulting Limited
TBC	Hotel Accomodation and Venue Finding	Capita Travel and Events
TBC	Soft Maintenance Services	Servest

POL00423684

POST OFFICE
AUDIT, RISK AND COMPLIANCE COMMITTEE

Accountable Person

Author: Tom Lee Sponsor: Alisdair Cameron Meeting date: 25 November 2019

Executive Summary

Context

This paper outlines the responsibilities of the Accountable Person ("AP"), in line with the principles of Her Majesty's Treasury's ("HMT's") Managing Public Money ("MPM"), and also describes how these responsibilities are being met.

Questions this paper addresses

- What and who is the Accountable Person at the Post Office?
- What are the responsibilities of the Accountable Person?
- How can we assess that these responsibilities are being met?
- What guidance is available for the Accountable Person?

6

Conclusion

The Accountable Person has a number of responsibilities which are focused around the key principles of the Government's Value for Money guidance, being:

- Regularity – ensuring adherence to legislation and regulations;
- Propriety – ensuring good governance;
- Feasibility – ensuring affordability and sustainability; and
- Value for money – ensuring value for the business and the exchequer as a whole.

Adherence against some of these requirements cannot easily be directly monitored and assessed due to the subjective and behavioural nature. However the current governance and reporting frameworks in place at the Post Office ensure many aspects are met. Examples such as the risk, internal audit, regulatory and secretariat teams ensure compliance around governance, and the internal financial reporting controls framework ensures adherence to the financial management requirements. Additionally specific requirements, such as signing the Annual Report and Accounts, including a governance statement, can be evidenced through formal signoff that has occurred.

Post Office uses its internal audit function and the findings of the external auditors to drive change and ensure internal systems of controls and governance are adequate. Value for money is controlled through regular monitoring and approval of spend through various review boards and routine reporting to UKGI. It is the AP's responsibility to ensure the requirements are met, however the information provided within this paper should allow appropriate assurances to be gained that the current organisational structure and processes in place provide adequate coverage. A report will be produced for the AP and ARC annually, outlining the rationale for why signoff can be performed on relevant formal documentation i.e. the Annual Report and Accounts.

Input Sought

The ARC is asked to note the current requirements around the Accountable Person's responsibilities and to comment on any concerns noted.

POL00423684

What and who is the Accountable Person?

1. There is no specific guidance made available by HMT which outlines what or who an AP is in respect of a non-departmental public body such as Post Office Limited ("POL").

2. Historical communication from UKGI to POL has stipulated that an AP can be considered the same as an Accounting Officer ("AO"), for which guidance exists. As such, for the remainder of this paper the term AP will be used, however the reference material for which decisions have been made have come from available guidance on AO's.

3. The AP is a singular designated individual within an organisation who is accountable for both the operations of the organisation and the preparation of its Annual Report and Accounts ("ARA").

4. The AP is usually the head of the organisation i.e. CEO, and is appointed by HMT.

5. The AP has changed within the POL over the past 12 months in line with changes at board level. However it should be noted that the person in role as at the time of signing the ARA is deemed to be responsible for the entirety of the period being reported on.

6. Individuals within role over the past 12 month period include:
   a) Paula Vennels – until resignation in April 2019.
   b) Alisdair Cameron – April 2019 until Sept 2019. AP for FY18/19.
   c) Nick Read – from Sept 2019

What are the responsibilities of the Accountable Person?

7. The AP is the individual who parliament call to account for stewardship of its resources i.e. they are deemed to have overall responsibility for the business they manage and will be held accountable for its performance and actions.

8. The primary responsibilities of the AP are outlined within the MPM guidance, which states that the AP should ensure the organisation abides by, and delivers on a number of defined standards designed to help meet the overall objective of the role. Further details are outlined in Appendix 1.

9. The key areas for which these relate are:
   a) Governance;
   b) Decision making; and
   c) Financial management.

10. Many of the standards required in the MPM represent desired behaviours and ways of working which are difficult to monitor and formally track. However the way the Post Office is designed and managed can help to ensure that these standards are met and therefore the role of the AP is delivered.

POL00423684

11. More formally, the AP is required to sign-off the ARA taking personal responsibility for delivery against the MPM standards. Within the ARA, the Governance section lists the key structures, actions and committees' in place that help to meet the desired standards of the AP.

12. When making key decisions or assessments, several standards can and should be used to assess whether the initiative meets the Value For Money ("VFM") guidance and therefore whether the AP can justify the decision to parliament reasonably as required. These standards are:

    d) Regularity and propriety – compliance with relevant legislation and ensuring good governance.

    e) Feasibility – Ensuring affordability and sustainability.

    f) Value for money – systematically evaluating relevant processes to ensure sustainability and value for the organisation and the Exchequer as a whole.

13. Other standards where the AP is held responsible include:

    g) Control – personally approve all Cabinet Committee papers and major initiatives.

    h) Management of opportunity and risk – achieve the right balance for Post Office's risk appetite.

    i) Learning from experience.

    j) Accurate accounting – ensure the ARA is correct and transparent, whilst recording the efficiency of the organisations use of resources.

14. The AP may be called to attend as a witness at the Committee of Public Accounts evidence sessions, which is not optional. The AP should report to Parliament accurately, meaningfully and without misleading them.

15. When the AP is unavailable for a significant period of time, the role should be deputised to another senior member, with any significant absences being highlighted to UKGI in order to appoint a temporary AP as required.

How can we assess that these responsibilities are being met?

16. In order to achieve the above, the AP should ensure adequate organisational structures, delegations of authority and management reporting tools are in place. Without these, it would be difficult for the AP to provide the assurance required to fulfil their responsibilities.

17. Given the nature of the AP's responsibilities, formal signoff to show adherence is not always possible. As such, many of the assurances gained are through review of the organisational structure and processes. The below outlines the key considerations that evidence that the AP's responsibilities are being met.

POL00423684

18. As evidenced within the 2018/19 ARA, the AP at the time, signed off the governance section of the ARA. Further, the ARA was approved by the external auditor and therefore the requirements around accurate accounting were formally met for the most recent financial year. Formal processes are in place to ensure the requirements are met annually.

19. POL regularly reports to UKGI on specific financial areas and has an internal Financial Planning and Analysis team who is responsible for governance around budgeting and forecasting across POL and reporting to UKGI as required. In addition to this, POL has a UKGI representative on the Board who is able to challenge and review decisions made by the AP and the Executive team.

20. The presence of a UKGI representative allows other key aspects, such as governance and decision making, to be routinely challenged and assessed ensuring the process of assessment against AP requirements is ongoing.

21. Across all levels of POL, governance frameworks are in place. For example, POL has terms of reference for Committees, there are clear levels of delegated authority and regular monitoring and reporting of risks to the Board which help the AP to make appropriate decisions.

22. Regarding the key components of VFM and risk appetite, review boards are in place, ensuring all significant spend within the organisation goes through a formal review and authorisation process. The structure, delegation of authority and key considerations should be, and are, routinely reviewed to ensure the requirements for the AP are being met. Financial processes are intertwined with these review boards to ensure actual spend is controlled in line with the governance framework.

23. POL has compliance teams in place to ensure regulatory requirements are adhered to across the myriad of environments to which it operates. Compliance is monitored and reported regularly to ARC as required.

24. POL's Financial Reporting Controls Framework is designed to mitigate the risk of fraud and error in financial reporting, thus providing assurances around accurate accounting and safeguarding assets.

25. CoSec also have a number of processes including place to allow formal monitoring of many of the above, whilst also ensuring specific requirements such as control over cabinet papers is adhered to.

26. Continuous review of reporting tools, organisation structures and governance frameworks is ongoing within POL, thus ensuring that areas of development are identified and improved as required. The ultimate driver is to ensure the requirements on the AP's organisation are met. The level of change seen within the organisation in recent years, and which is still ongoing, is evidence of this focused development.

POL00423684

27. On an annual basis, a report will be provided to the AP and ARC to provide rationale as to why the AP can signoff on relevant formal reporting i.e. the ARA. Finance will be accountable for producing the report, however input will be required and sought from relevant teams across POL including Legal, Compliance and Company Secretariat with relevant legislation and guidance being taken into account.

What guidance is available for the Accountable Person?

28. There are a number of resources available, which have been used in the creation of this report. The key documents to refer to, and which are available on the government website, include:

a) Managing public money.
b) The accounting officer's survival guide.
c) Making an accounting officer assessment.

POL00423684

Appendix 1 – Standards expected of an Accounting Officer's organisation, per latest "Managing Public Money" guidance

Box 3.1: standards expected of the accounting officer's organisation

Acting within the authority of the minister(s) to whom he or she is responsible, the accounting officer should ensure that the organisation, and any ALBs it sponsors, operates effectively and to a high standard of probity. The organisation should:

governance

- have a governance structure which transmits, delegates, implements and enforces decisions
- have trustworthy internal controls to safeguard, channel and record resources as intended
- work cooperatively with partners in the public interest
- operate with propriety and regularity in all its transactions
- treat its customers and business counterparties fairly, honestly and with integrity
- offer appropriate redress for failure to meet agreed customer standards
- give timely, transparent and realistic accounts of its business and decisions, underpinning public confidence;

decision-making

- support its ministers with clear, well reasoned, timely and impartial advice
- make all its decisions in line with the strategy, aims and objectives of the organisation set by ministers and/or in legislation
- take a balanced view of the organisation's approach to managing opportunity and risk
- impose no more than proportionate and defensible burdens on business;

financial management

- use its resources efficiently, economically and effectively, avoiding waste and extravagance
- plan to use its resources on an affordable and sustainable path, within agreed limits
- carry out procurement and project appraisal objectively and fairly, using cost benefit analysis and generally seeking good value for the Exchequer as a whole
- use management information systems to gain assurance about value for money and the quality of delivery and so make timely adjustments
- avoid over defining detail and imposing undue compliance costs, either internally or on its customers and stakeholders
- have practical documented arrangements for controlling or working in partnership with other organisations, as appropriate
- use internal and external audit to improve its internal controls and performance.

6

POL00423684

POST OFFICE LIMTIED
AUDIT, RISK AND COMPLIANCE COMMITTEE

Commercial Partner Contingency Paper (McColl's)

Author: Karl Oliver Sponsor: Amanda Jones Meeting date: 25th November 2019

Executive Summary

Context

As follow-up to our previous paper, this paper provides an update on the monitoring of the financial stability of our multiple retail partners and McColl's specific contingency planning activity.

Questions this paper addresses

- What is our monitoring telling us?
- What is the total risk?
- What are the potential scenarios?
- What are our plans to mitigate?
- What are the next steps?

7

Conclusion

- We have one large partner at an increased risk of financial instability, McColl's.
- The McColl's PO estate is made up of 615 (+27 outreach) branches, serving 600k customers a week, generating £32m of POL income p.a.
- Any significant closure in the number of McColl's Post Offices would put maintaining 11,500 branches at risk. Any drop significant/sustained drop below 11.5k branches world require formal engagement with government.
- From the review of the McColl's estate there are 82 branches that we would prioritise based on vulnerable customer access.
- Whilst we have modelled and proposed outcomes at branch level for all branches, further branch level activity is required to validate the modelling, scope alternative solutions and generate detailed local plans for each prioritised branch.
- Our next steps are to commence building those plans immediately after our peak Xmas period (early January).

Input Sought

An opportunity for the committee to ask questions and feed into the next steps.

POL00423684

The Report

What is our monitoring telling us?

1. Our existing monitoring highlights that McColl's is the only large partner with a heightened risk of financial instability. McColl's are our largest partner with c.615 Post Office and 27 outreach branches within their estate.

2. In response to questions from ARC, we explored Thomson Reuters subscription software that provided additional metrics (credit, market sentiment, loan notices, etc). Following a discussion with our CFO, we decided that whilst the insight was of use it would not change our actions significantly and so have not taken up the subscription (cost of c.£19k p.a.)

What is the total risk?

3. Customer
   The McColls PO estate currently serves c.600k customers per week (31.5m p.a.). Within this estate there are 82 branches that we would prioritise for replacement based on 'vulnerable' customers and accessing of PO services. This is made up of:
   a. Nearest branch > 1 mile away from an urban deprived area (26)
   b. Rural branches > 3 miles away from nearest branch (26)
   c. Urban branches > 1.5 miles away from nearest branch (30)

4. Political
   We are tasked with maintaining a minimum network number of 11,500 branches. Any significant drop below these numbers for a sustained period would require that we notify government formally. There would be a minimum expectation of a detailed recovery plan and plan to avoid this situation arising in the future. Whilst there is no penalty for dropping below these numbers in place, government would need to be seen to be taking action.

5. Financial
   Using 18/19 FY figures, McColl's Post Office estate generated c.£32m of Post Office income from their 600+ branches, with total remuneration of £19m. Considering a worst case scenario where all of these branches close and Post Office sought to replace all of them the cost of replacement would be c.£24m. From experience approximately, 50% of this business would be retained if these branches closed, migrating to neighbouring branches.

What are the potential scenarios?

6. Appendix 1 summarises the scenarios and our response to each in the event of a partner becoming financially unstable. Ranging from the partner raising capital, through asset/store sales through to insolvency.

Commented [KO1]:
Commented [KO2]:
Commented [KO3R2]:
Commented [KO4]: We've used 53% historically (calculation for state aid)

7

POL00423684

What are our plans to mitigate?

7. The operational plan focuses on re-opening branches in existing locations, working with administrator, the prioritised branch list and temporary operators to re-establish service. Where re-openings are not possible or de-prioritised, the focus will be on maintaining alarms, gaining access and co-ordinating audit & cash teams to allow a prioritised defunding of the sites.

What are the next steps?

8. Following the peak Christmas period, using the prioritisation described above, build a detail branch level local action plan to secure services for each of these locations.

7

POL00423684

Appendix 1 – Partner Failure Plan

1. Background

Commercial partners operate approximately 2,200 Post Offices (19% of the 11,500 PO estate); 25 Partners have 10 or more branches, however, the 5 largest partners operate c.1,300 branches (11% of the 11,500 PO estate) which exposes us to a potentially significant risk to service if any of these larger partners were to get into financial difficulty.

We are currently undertaking a review of our strategic partnerships and this review will consider the question of 'balance of the estate' between independents and commercial partners to evaluate our risk exposure, including whether there should be a cap on the number of Post Offices within a single partner estate.

This paper describes our contingency plan in response to a commercial partner getting into financial difficulty and the resulting risk of closure of PO branches. It identifies potential scenarios, assesses the options available to the Post Office (PO) and uses highest impact on PO branch numbers as the key prioritisation metric. Our priorities are to:

1. Continue to provide PO services within communities, including fulfilling our responsibility to vulnerable customers, classified in line with GLO response plan as:
    a. Nearest branch > 1 mile away from an urban deprived area
    b. Rural branches > 3 miles away from nearest branch
    c. Urban branches > 1.5 miles away from nearest branch
2. Minimise financial loss to the PO
3. Create a plan that can be adapted in the event of a similar occurrence with any commercial partner who operates POs

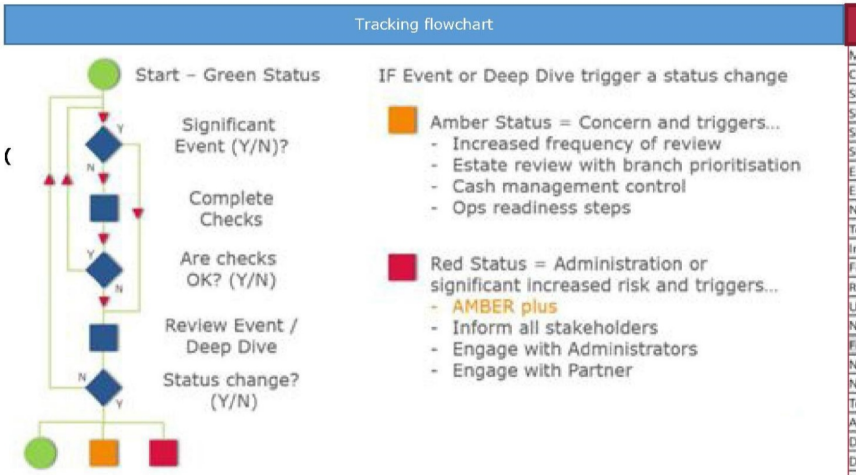
POL00423684

2. Monitoring Process

A Partner monitoring process has been set up since the beginning of FY19/20 and is produced monthly. Following a change in status, additional checks on the PARTNER will remain in place until we are satisfied the situation has stabilised.

Key metrics include Experian credit checks; share price tracking and Net Debt vs EBITDA – KPIs in table below.

In addition to the tracker established internally from 'free to access' data we have explored subscription to a specialist analysis platform. Post Office has previously subscribed to the EIKON platform which incorporates the measures within our tracker plus a broad range of alternatives including big 4 creditor scoring and 'News trending/sentiment' analysis. Our recommendation, following conversation with CFO is that we do not resume our subscription. (The estimated cost is £19k+vat per year - includes broker report access).



KPIs on tracker
Market Cap (£)
Current Share Price (0.00p)
Share price high (L12M) (0.00p)
Share price low (L12M) (0.00p)
Share price % change (L12M)
Share price % change (L3M)
Experian Delphi Score (out of 100)
Experian Odds of Failure
Net Debt/EBITDA
Total Debt/Equity
Interest cover (Earnings/int.exp)
Financial Year End
Recent Announcements
Upcoming announcements
Notes
Finance (RAG)
Number of Company operated POs within estate
Number of Symbol operated Pos within estate
Total of whole estate
Acquisitions Company operated (L12M)
Disposals Company operated (L12M)
Disposals of PO with retail retained CO (L12M)
POL Income (notional) (£) YTD
POL Income variance YoY & YTD (%)
Reported PO P&L (if applicable)

POL00423684

3. Monitoring Triggers

What are the likely events or potential triggers that might indicate a partner is in financial difficulty?

1. The Group is unable to pay its debts
2. Its liabilities exceed its assets
3. The Group has breached or expects to breach its banking covenants

Through the monitoring mechanisms outlined in point 3, we anticipate being able to have foresight of these indicators to enable us to trigger our response plan.

What are the possible outcomes if one or more of the triggers above materialise?

1. Renegotiation of funding or fund-raising via sale of assets
2. A mergers and acquisitions (M&A) process – where the Group seeks buyers to purchase part or all the portfolio. This sale could be achieved via a pre-pack administration
3. An administration – which may include trading the stores whilst seeking a sale or effecting an immediate closure of the stores
4. A liquidation of the Group.

4. Post Office Response

How might each of these outcomes play out in terms of different scenarios?

Partner Outcomes	No	Scenarios
Recovery	1	Partial sale of estate
M&A (pre-pack)	2	Whole estate is acquired by a favourable 3rd party
	3	Whole estate is acquired by an unfavourable 3rd party (or parties)
Administration	4	Partial acquisition + closure of some sites (favourable 3rd party)
	5	Partial acquisition + closure of some sites (unfavourable 3rd party)
	6	PO acquires all sites with Post Offices within store
Liquidation	7	Whole estate is liquidated

POL00423684

For all 'administration/insolvency scenarios'
In each scenario where the company goes into administration, there are several steps that are common which include:

- Stand-up cross-functional team (representation from Retail Operations, External Comms, Legal, Audit, Cash Management, Security, NDA, Property, Finance, Agents Remuneration, Business Continuity) and trigger each function 'response plan' as appropriate
- Contact administrator to assert our rights over PO cash and assets and agree access to any closed sites for either decommission or temporary operation
    - Ensure administrator acknowledgement of security requirements for PO cash and assets
    - Plan with the administrator to open sites as 'PO only' or gain access to defund the sites
- Instigate operational plan for 'entering' admin & any closures, which includes arrangements for 'continuous trading'
    - The operational plan focuses on re-opening branches in existing locations, working with administrator, prioritised branch list and temp operators to re-establish service.
    - Where re-openings are not possible or de-prioritised, the focus will be on maintaining alarms, gaining access and co-ordinating audit & cash teams to allow a prioritised defunding of the sites

How would Post Office respond to each Scenario?

No	Scenario	Likelihood of Post Office closures				Risk description	PO Response
		Imme-diate	Short <6m	Mid 6-12m	Long 12m+		
1	Partial sale of estate to 'fund raise'	L	L	L	L	Could range from simple BAU 'commercial transfer' activity through to variations of scenario 2 & 3. Likely to be a 'part' of their PO estate (rather than whole) and likely to be 'sold' as going concern. Risk is therefore likely to be lower numbers and lower risk of closure.	• Engage with buyer to gauge appetite for continued operation of PO's instore (Is having a PO in store aligned to the buyer's strategy?) • Work with buyer on any estate review to... i. ensure PO retained or relocated ii. identify PO/a PZ opportunities in new estate if appropriate • Establish PO view of new position for acquirer i.e. is size of estate within guide and are they financially stable – this should determine PO on-going activity

POL00423684

No	Scenario	Likelihood of Post Office closures				Risk description	PO Response
		Imme-diate	Short <6m	Mid 6-12m	Long 12m+		
						Overall risk: LOW	• Trigger legal and contractual work to novate existing contracts to new partner as appropriate (aiming to achieve continuity of service)
2	Whole estate is acquired by a favourable 3rd party	L	L	M	H	Retailers 'new' combined estate could have duplication of sites within a single location – this could lead to closures/disposals (e.g. When McColls acquired subset of Co-op estate) Any estate review is likely to be 12-24 months post acquisition and 'sale' rather than closure is likely preferred option for retailer Transition to NEW partner as Pre-pack or following trading admin would be expected to be smooth (continuous service). Overall risk: LOW	• Engage with the administrator and/or buyer to gauge appetite for continued operation of PO's instore (Is having a PO in store aligned to the buyer's strategy?) • Work with partner on any estate review to... i. ensure PO retained or relocated ii. identify PO/PZ opportunities in new estate if appropriate • Establish PO view of new position for acquirer i.e. is size of estate within guide and are they financially stable – this should determine PO on-going activity • Trigger legal and contractual work to novate existing contracts to new partner as appropriate (aiming to achieve continuity of service)
3	Whole estate is acquired by an unfavourable 3rd party (or parties)	M	M	H	H	Immediate branch closures are flagged as MEDIUM risk as there will be no obligation to serve notice on any acquired sites but establishing new retail estate is likely to be prioritised and retailer is likely to be mindful of stakeholder backlash to wholesale PO closures Mid to Long-term closures have a HIGH likelihood and potentially with high volume (depending on PO partner estate) Disposals likely to be a mix of... i. PO closed with retail retained ii. Whole site put up for sale or closed	• Engage with the administrator and/or buyer to gauge appetite for continued operation of PO's instore e.g. Is having a PO in store aligned to the buyer's strategy? – assumed 'not aligned' in this scenario • Engage with acquirer to secure 'immediate' continuation of PO trading and if required agree PO disposal plan (likely to require investment and any solution is likely to be time-bound) e.g. overpayment in exchange for 12m guarantee on existing estate & requirement upon PO to dispose of X stores per 3 months • Review Partner estate for alternative service solutions i.e. Can PZ/Parcelshop help to retain or replace Post Offices? • Establish PO view of new position for acquirer i.e. is size of estate within guide and are they financially stable – this should determine PO on-going activity • Trigger legal and contractual work to novate existing contracts to new partner as appropriate (aiming to achieve continuity of

POL00423684

No	Scenario	Likelihood of Post Office closures				Risk description	PO Response
		Imme-diate	Short <6m	Mid 6-12m	Long 12m+		
						Continuous trading may not be an option with 'unfavourable partner' even with incentivisation. Overall risk: HIGH	service), including any fixed-term agreements (can be protracted where partner is renegotiating all existing core business contracts)
4	Partial acquisition + closure of some sites (favourable 3rd party)	H	H	M	L	Immediate and short-term closure of branches has HIGH likelihood. In this scenario the administrator has secured the sale of one or more subsets of the estate to one or more acquirers. Subsets may have been broken in to 'profile' (e.g. based on turnover/size of store/proposition) or negotiated in groups with acquirer (e.g. acquirer cherry-picks the sites that they are interested in). With maturity of sector and high appetite for strong convenience sites it is more likely to be 'cherry picking'. This is favourable to PO as acquirer will only be picking up sites that they expect to retain (no duplication of estate) so Mid and Long-term risk decreases High volume of closures will leave significant PO funds and assets on site with difficulty accessing/alarm switch-off etc. Cost to temporarily run 'closed' branches will exceed remuneration.	• Engage with the administrator and/or buyer to gauge appetite for continued operation of PO's instore (Is having a PO in store aligned to the buyer's strategy?) • Work with partner on any estate review to... i. ensure PO retained or relocated ii. identify PO/PZ opportunities in new estate if appropriate • Establish PO view of new position for acquirer i.e. is size of estate within guide and are they financially stable – this should determine PO on-going activity • Trigger legal and contractual work to novate existing contracts to new partner as appropriate (aiming to achieve continuity of service)

POL00423684

No	Scenario	Likelihood of Post Office closures				Risk description	PO Response
		Imme-diate	Short <6m	Mid 6-12m	Long 12m+		
						Transition of estate acquired by favourable partner expected to be smooth (continuous trading). Overall risk: HIGH	
5	Partial acquisition + closure of some sites (unfavourable 3rd party)	H	M	H	H	Follows scenario 3 but with greater risk of immediate closures. High volume of closures will leave significant PO funds and assets on site with difficulty accessing/alarm switch-off etc. Cost to temporarily run 'closed' branches will exceed remuneration. Overall risk: HIGH	(See scenario 3)
6	PO acquires some/all sites with Post Offices within store	L	L	L	L	PO acquires some or all sites with a Post Office securing on-going PO services at the location PO would be acquiring an estate that no other retailer or private equity specialist turnaround company chose to acquire (indicating financial issues are more significant) – assumes that we are last option PO are NOT retailers and are not currently set up to manage a separate retail estate (i.e. would require external resource/expertise) which coupled with the above further compound financial issues through increased cost	• Identify 'funding options' (emergency funding) • Review existing estate to allow segmentation and prioritisation for 'acquire for continued service' or 'advertise opportunity' to include... i. Vulnerable customer branches ii. High POL income branches iii. Low value/impact branches • Establish 'waiting list' for permanent opportunities (aligned to segmented list above) e.g. have people 'lined-up' for POL to flip the branches back to 'independent Post Masters' with POL as landlord • Pre-work - workout costs/alternative views to include... i. Estimated Outcome Scenario (EOS) built – indicator of 'whole estate' value ii. Estimate 'replacement costs' for rebuilding estate LFL

POL00423684

No	Scenario	Likelihood of Post Office closures				Risk description	PO Response
		Imme-diate	Short <6m	Mid 6-12m	Long 12m+		
						PO would have no supply agreements in place and would need to negotiate a supply agreement (unlikely to be more favourable than previous agreement as subset of original estate) PO would have no IT infrastructure or contracts in place for the retail operation (ePOS, finance, connectivity, payroll, reporting, etc) with option to continue to operate 'as is' unlikely and/or increased costs. LFL replacements likely to be a tailored/closed system (not off the shelf) PO would have no property leases in place. Whilst there would be potential to renegotiate costs this would tie PO to mid-long-term leases. PO would TUPE existing staff across – IF acquisition was to allow continued PO services whilst managing the 'sale'/disposal of sites, PO would have cost exposure for redundancy etc. Overall risk: HIGH	iii. Estimate 'by design' replacement (which we'd put in place if starting from scratch) iv. Include lost revenue and likelihood of replacement v. Include any benefits of 'by design' estate (i.e. mains to local cost and remuneration) • Establish 'senior decision' team and ways of working • Identify external support functions to include... i. Insolvency Administrator (advisory) ii. Corporate finance support – access to funds iii. Surveyors/valuers to establish value of estate iv. Legal contract due diligence and company set-up • Set-up 'new' company to operate sited through and complete initial engagement with stakeholders including... i. Suppliers – Establish accounts and ii. Credit insurers – give comfort on ability to pay iii. Other insurers – warranty and indemnity insurance iv. Landlords – • Manage trade marketing (immediately upon appointment) to include
7	Whole estate is closed and/or liquidated	H	H	H	H	All sites closed by administrator. This could precede continued negotiation or insolvency. Cost to re-open sites 'temporarily' will exceed remuneration. High volume closures will leave significant PO funds and assets on site	See steps for all scenarios

POL00423684

No	Scenario	Likelihood of Post Office closures				Risk description	PO Response
		Imme-diate	Short <6m	Mid 6-12m	Long 12m+		
						with difficulty accessing/alarm switch-off etc. Overall risk: HIGH	

Next steps

1. Continue to finesse the detailed operational plan at function level to underpin the responses outlined above
2. Set-up 'Scenario-gaming' workshops for cross-functional team to test response plans and discuss validity of scenario

POL00423684

Risk, Compliance and Audit Report

Author: J Ellwood, J Hill, J Appel Sponsor: Al Cameron/Ben Foat Meeting date: 25 November 2019

Executive Summary

Context

An update on the key and emerging risks and compliance matters that Post Office is managing and an update on the latest Audit position.

Questions this paper addresses

- What are the key risks and compliance matters and what is the business doing to address these?
- How is the Risk Framework maturing?
- What is the status of the Change Portfolio and its current top portfolio risks and key delivery challenges?
- What progress is made with delivery of the Internal Audit programme and completion of audit actions?

8

Conclusion

- The paper provides an update on the following top risks: PCI, IT Technology and Interruption, People, Business Continuity, Payzone and Brexit. **Appendices 1, 2 and 3** in the reading room provide more detail. We also maintain a watching brief on the Telco text relay OFCOM investigation.
- The Risk Policy has been restated and approval is sought in a separate paper. The Risk Management Framework has been reviewed and refreshed. A copy is provided in **Appendix 4** in the reading room. The Archer Risk module technical 'Go Live' remains on track for November and UAT is currently underway.
- The overall Change Portfolio performance remains Amber with 8 projects reporting an overall (or elements of) Red RAG. This is an increase of 4 since the previous report. **Appendix 5** in the reading room provides more detail.
- The number of change risks under management through the ServiceNow application stands at 407 across 10 business portfolios. Retail Products (97) and IT Platform (75) have the highest proportion of active risks.
- Ofcom has indicated that the text relay enforcement case remains open to reaching a settlement with us rather than moving straight to applying a penalty. We expect to hear from Ofcom in November on the next steps.
- The number of high value and complex cases relating to banking deposits continue to increase and we are cooperating with different law enforcement bodies and the banking partners to increase our understanding and to mitigate financial crime.
- Branch Mystery Shopping results continue to show poor conformance for the Travel Insurance sales process. Messaging on Horizon has been updated and we continue to seek feedback from the branches to understand why colleagues may not be following process.
- A number of branches that recently requested to be able to sell Travel Insurance have not completed their mandatory training, which includes Telecoms training as it reinforces customer care. If these branches have not completed their training by 30th November their ability to sell Travel Insurance and Telecoms products will be removed.

POL00423684

- Internal Audit have completed 11 reviews since the September ARC meeting (9 POL and 2 POI). There are currently no overdue audit actions.
- A review of the 2019/20 Internal Audit programme indicated that the number and focus of the reviews on plan are still appropriate and we recommend only one change at this time (par. 3.8).

Input Sought

The Committee is requested to note this paper and approve the proposed changes to the 2019/20 Internal Audit plan.

The Report

Risk

Author: Jenny Ellwood

What are the key risks facing the business and what is being done to address these?

8

1.1. Legal & Regulatory and Strategic are the principal risk categories which continue to report Red within the Heatmap (see Appendix 1). The People principal risks have deteriorated due to the increased likelihood of industrial action during Christmas. The spans and layers review work also raises a risk of loss of corporate memory.

1.2. The top Post Office risks are shown in Appendix 2. The Cyber Threat risk has reduced in light of the DLP pilot, enhanced capability of the SOC information security forums and addressing the key Deloitte Audit findings. IT Technology and Business Interruption risk has reduced from Red to Amber following (i) a successful failover test from Fujitsu's primary to its secondary datacentre, (ii) Verizon successfully performing a number of DR tests and, (iii) Computacenter confirming installed outdated software will not adversely impact system recovery time should there be a major incident. This will be verified in a workshop planned for November.

1.3. PCI remains a key Legal & Regulatory risk and the score remains unchanged (4:4). The programme consider the position is improving. Pin pad rollout has commenced and is progressing to schedule. Significant progress has been made with Ingenico and Fujitsu who confirm firm timelines and costs will be provided by this month. We have a plan to November and we are tying down the costs and details with suppliers.

1.4. The Business Continuity risk likelihood score has reduced from 4:3 to 4:2 because of site testing performing in line with agreed plans.

1.5. In relation to FS&T, we are maintaining a watching brief on Telco text relay, which remains a risk. A status update is covered in the Compliance section of the paper.

1.6. In September the Payzone Bill Payment Ltd Board agreed the Risk Impact and Likelihood matrix (Harm Table) and that any risk scoring 12 or above, would be outside of their appetite and escalated to Board for visibility and monitoring. Post

POL00423684

Office continues to support Payzone in the development of a wider Risk Management Framework, Risk Appetite statements and enhanced Risk Register. A copy of the Payzone heatmap is provided in Appendix 3.

1.7. The Payzone risk which was sensitive at a Group level and progress in mitigating it is set out below:

Risk	Mitigation Plan	Current Score using Payzone I/L	Current Score using POL I/L
The urgency in deploying a permanent fix for an existing terminal pairing issue (between devices E200 and T103) affecting agent and customer transactions may increase with on boarding of high profile clients. If agents are unable to carry out the transactions there will be significant impact to customers, particularly vulnerable.	Following the on-boarding of a dedicated contractor, significant progress has been made on defining the issues (mainly around Terminal pairing and WiFi connection). 1st software update fix has been released to the high problem sites. Promising initial feedback WiFi connection strength is being investigated. Identified software bugs can be fixed and issues remediation is ongoing with completion planned before 1/2019 go-live.	20 (4:5)	9 (3:3)

1.8. The EU have agreed a Brexit extension to 31 January 2020, with the option for a deal to be agreed before this date if possible. A General Election has been called for 12 December. Both these events have led to 2 emerging risks:

- The 2nd Withdrawal Agreement considers Northern Ireland to be part of the Customs Union. The Mails process may need to change as post between the UK and NI may now require custom forms. Horizon may also need to allow for multiple VAT rates (as NI may need to align with the Eire, rather than UK, VAT regime);
- A General Election may bring in a Government with a different policy position on the Post Office

8

1.9. The emerging risk previously highlighted around Barclays withdrawing from offering their customers the option to withdraw cash from the Post Office network has been resolved. Barclays have reversed their earlier decision.

How is the Risk Framework maturing?

1.10. The Risk Policy has been restated for approval. A supporting Risk Management Framework has also been developed (see Appendix 4). Both documents are to be communicated to the business and be accessible from the Central Risk intranet site.

1.11. Deloitte carried out an advisory review of Phase 1 of the Archer development work. It confirmed current Phase 1 configuration and development is satisfactory to progress to UAT. Technical go live remains on track for November. All findings raised in relation to Phase 1 have been actioned. The outstanding actions relate to future phases with their acceptance dependent on the level of future maturity we seek to achieve.

1.12. Work continues to improve quality of change risks captured in Service Now with the introduction of risks and issues guidance as well as, worked examples provided to the change community. Analysis has been undertaken to identify risk themes. Project execution and financial management have the most risks.

POL00423684

What is the status of the Change Portfolio, its current top portfolio risks and key delivery challenges?

1.13. The overall status of the portfolio remains Amber. A 'pause' on new funding requests has been put in place by the Investment Committee (IC), until Mid-November. We expect re-forecasting in the light of the freeze, the interventions on individual projects and the wider prioritisation work to reduce spend this year to within budget

1.14. The portfolio has seen a material reduction in the number of projects reporting Amber Risk RAGs. This has resulted in the portfolio risk RAG status being downgraded from Amber to Green which, in turn, has contributed to the portfolio status remaining at Amber.

1.15. There has been an increase in the number of Platinum/Gold projects reporting an overall Red RAG status which reflects both proactive and targeted reviews of projects and a churn in which projects are reporting red as projects previously at risk are brought within acceptable tolerance or deliver/close. Only PCI compliance remains red from July. We believe earlier mechanisms for reporting risk are helping to highlight and resolve risks and such churn will continue. The 8 projects (from a total of 35) currently reporting an overall (or elements of) Red RAG status are:

- PCI Compliance (Overall Red RAG)
- Developing Capabilities (Delivery Red RAG): This project is working to provide Regional and Area managers will skills and tools to build trusted relationships with Postmasters. PowerBI and Scheduling Tool development the reason for Red RAG due to dependence and non-delivery from Project Arrow. Full solutions unlikely to delivered in 2019/20 so manual workarounds will be required in the short term.
- Postmaster Application process (Delivery Red RAG): Further penetration testing is required linked to GDPR compliance, delaying go live for Run-a-Post-Office (RaPO) and Electronic Business Plans (EBPs). Project are hoping for November delivery, before the change freeze.
- Self-Service Portal (Branch Hub) (Delivery & Overall Red RAG): Re-plan underway to address development output and cadence, benefits and business readiness. Board update on options to be presented.
- EUM (Common Services) (Costs, Delivery, and Overall Red RAG): Completion delayed until end October by issues with final deliverables. Costs expected to exceed approved budget by around 2.5%.
- IDS Digital Identity (Delivery, Risk, and Overall Red RAG): Module 1 delivery in April 2019 not achieved. 6 months behind schedule. Digidentity must carry out major 'rework'. Delivery confidence is low.
- Digitising Mails (Cost & Overall Red RAG): Reporting Red as spend is on hold while business evaluates various delivery options.
- Belfast Exit (Overall Red RAG): Business has stated desire to urgently restart the programme in time for Oracle's end-of-life in December 2020 and will start replacing the work, within agreed budgets in November.

1.16. Appendix 5 within the reading room provides a summary of the current key 'Platinum and Gold' change programmes and their current reporting status.

POL00423684

Compliance Author: Jonathan Hill

Telecoms

Text Relay

2.1 We responded to Ofcom's second S135 information request with a response that included 191 emails. At a meeting on 24th September Ofcom challenged the picture of events portrayed by these emails and our S135 response compared to the understanding it had drawn from our early correspondence. Ofcom sought clarification on the differences to which we responded on 4th October.

2.2 Ofcom contacted us on 30th October to give us an early, informal update on its decision. As a result of our 4th October submission, Ofcom has indicated it remains open to reaching a settlement with us rather than moving straight to applying a penalty, which would have been very severe and include a significant investigation.

Mystery Shopping and Telecoms Branch Training

2.3 We are now reporting Telecoms Mystery Shopping results, following increased focus from the regulator on all providers and their sales approaches. As we are experiencing in the wider FS and Insurance products sales, the key issue is one of conformance with the sales process in branch, particularly giving customers their internet speed information, which is on Horizon.

- We are folding remediation activity into the general improvement activity for Insurance products as set out in paragraph 2.33.

2.4 Telecoms training is required for all branches engaging in Telecoms sales. However, as part of the insurance IDD requirements, which includes 15 hours of CPD per year, it was agreed with POI that the telecoms training module could count towards the IDD CPD target. The request from 525 branches to be allowed to sell Travel Insurance, who went live in August, meant that these branches are required to complete telecoms training too. 131 of these branches have not completed their telecoms training.

- We have agreed with Network that any branch where mandatory training (including insurance and/or telecoms) has not been completed by 30th November 2019 will be turned off from being able to carry out insurance and telecoms product sales.

Fairness Principles

2.5 Following the singing up to Ofcom's "Fairness" principles along with the rest of the industry earlier in 2019, we are meeting Ofcom in December to discuss how we are meeting/intend to meet them. This is part of Ofcom's approach to address the "Loyalty Penalty" super complaint.

Regulatory Diary

2.6 The Telecoms Regulatory Calendar for October 2019 is provided as supplementary information (Appendix 6).

Data Protection

GDPR Contract Remediation – please refer to separate agenda item

British Gas

2.7 Good progress is being made with the British Gas project. The Privacy Impact Assessment (PIA) for POL has been completed and sign off is expected before 'go live'.

8

POL00423684

Data Protection Breach – Post Office Insurance

2.8 An employee used company personal data without authorisation for MBA research purposes. The individual was disciplined and reminded of the data protection obligations. This breach was reported to the ICO as per statutory requirements. Post Office received notification from the ICO that no further action would be taken and commented that the remediation implemented are examples of good practice.

Changes to Post Office "Cookie" Management

2.9 Recent changes to guidance and the development of case law requires Post Office internet sites and Apps to be updated. These changes will significantly impact on the quality of data and commercial value of the information we receive regarding customers and perspective customers. A new Cookie Policy is being written and due for release in Q4.

2.10 Communications are being prepared to be sent out by the Compliance Director to impacted businesses. Implementation plans are currently in progress with an expectation that the changes will be implemented in Q3/4.

Financial Crime

Compliance with Money Laundering Regulations

2.11 Between 6th September and 27th October 2019, 88 new Bureau de Change non-conformance cases were identified in comparison to 82 during the same period in 2018. We expect this level of annual increase to continue and accelerate as we implement additional Bureau de Change monitoring reports.

2.12 Between 6th September and 27th October 2019, there were 17 non-conformance cases relating to customers who had purchased in excess of €15K in 90 days. This volume is consistent with the same period in 2018. Mitigating actions have been taken and the individuals have been reported to the authorities where required.

2.13 There was one material breach in September, relating to a customer who purchased c. £38K in foreign currency at 12 different branches in East London. The linked transactions have been reported to the authorities. Purchases were made using two debit cards, one UK issued and one Dutch issued. The UK bank has been contacted and they advised they would investigate further. All branches concerned were contacted and network communications issued to the targeted areas - the activity subsequently stopped.

2.14 In branch (on demand and pre order) Terms and Conditions have been approved and published on the Internet by the Travel Money Team. This will enable the Financial Crime team to write directly to customers who breach the £10k over 90 day's threshold.

2.15 The fix for outstanding AML Credence data integrity architecture issues that are impacting Bureau de Change has been delivered by Accenture, and these have been tested in AML Credence and the Business Objects reports are currently being re-written. This fix should resolve the outstanding issues, reduce current false positives and enable further reports to be introduced. The fix to address the Sanctions match data gap has not worked and a live service incident has been raised to identify why the data is not appearing in AML Credence. This data is needed so that further checks can be undertaken, and if necessary, the attempt by the Sanctioned individual can be reported to the Office of Financial Sanctions Implementation (OFSI).

POL00423684

Anti-Bribery and Corruption ("ABC") update.

2.16 The annual ABC training was scheduled 6th – 30th September. As at the end of September c.86% of employees had completed the training and test as required. As at 22nd October 2019, this had increased to 95%. The survey that accompanied the training was completed by over 1200 individuals and indicated that they were confident to apply the training in their roles that was delivered this year.

2.17 Since the training, we have seen a slight increase in reporting and have received a number of queries into the G&H inbox, indicating that staff are following the guidelines. A new reporting and approval portal is currently being built, with improved workflows and reporting that should aid conformance. Delivery is expected during Q4.

Whistleblowing update

2.18 No significant issues to report. Communication activity is planned for the rest of the year to raise awareness.

Fit and Proper

2.19 Following the August meeting of the Declaration Oversight Committee, 760 branches that had not provided complete F&P declarations had their ability to transact Travel Money and Moneygram removed between 6th and 13th September.

2.20 Since then, we have run a weekly reinstate batch for agents who have subsequently returned their documentation, protecting a further c£1.1m of income p.a.

2.21 On 12th October, the remaining 186 non-compliant branches (accounting for less than £250K POL income) were advised that their premises were to be de-registered with HMRC. Subsequent provision of F&P data post de-registration may result in reinstatement but this will not be immediate as each branch will have to be reviewed and re-registered.

2.22 As at 13th November, 100 branches remained non-compliant and the file to de-register the premises with HMRC will be processed and sent week commencing 18th November 2019.

2.23 The fix to remove pre-order from de-registered branches from Atos will not go live until early 2020. Currently there are manual checks in place for the revoked branches, but for the de-registered branches, FRES can put a fix in their systems to permanently remove pre-order capability. It has been identified that branches in a revoke status can still undertake buy-back transactions, and a fix for this is being pursued.

2.24 Some data gaps have been identified retrospectively and are currently being investigated. These need to be resolved before we present to HMRC a full premises registration list with the relevant agent data appended on 22nd November 2019. Data gaps in relation to new and temporary agents are being addressed with the on-boarding teams and the processes for data capture are being reviewed to ensure that sufficient managerial controls exist to ensure that policy requirements are adhered to.

2.25 The BAU solution for agent data changes to be sent to HMRC each month, having received Enterprise Architecture Group approval is now due to go to Portfolio Review Board on 19th November to secure funding. The planned go live for the BAU solution is the first week of April 2020.

2.26 Current structural changes across the business are not being effectively impact assessed by or communicated to the Compliance team to ensure that appropriate HMRC Fit & Proper tests are completed in accordance with regulatory requirements – this includes the removal from HMRC records of individuals

8

POL00423684

moving to non-designated roles or leaving the business. The Joiners Movers Leavers project should close this gap. The current list of impacted roles will be reviewed, refreshed and submitted to the January 2020 RCC for approval.

Regulatory updates

2.27 The EU Commission produced a report for the European Parliament and The Council on the 2017 supranational risk assessment of money laundering and terrorist financing risks affecting the internal market and relating to cross-border activities. Within this report one of the main risks identified was cash and cash-like assets, which remains criminals' instrument of choice to move funds rapidly from location to another. The Cash Control Regulations (applicable from June 2021) extend the obligation of any traveller entering or leaving the EU and carrying €10,000 or equivalent in cash to declare it to Customs. It also extends the definition of cash to include other instruments or highly liquid commodities, e.g., cheques and prepaid cards.

2.28 The 5th Anti-Money Laundering Directive is still scheduled to be transposed into UK law by January 2020, and will further enhance the Money Laundering Regulations. This will include limiting anonymity offered by virtual currencies, wallet providers and pre-paid cards. For example, the One4All gift card maximum value will need to be reduced to a maximum of €150 equivalent if it is to continue to be sold as an anonymous card.

External Threats: HMRC record fines on MSBs

2.29 On 4th September 2019, HMRC announced a record fine of £7.8m against Touma Foreign Exchange Ltd, a Money Service Business (MSB) based in West London. It had breached the Money Laundering Regulations between June 2017 and September 2018, including failures within its F&P tests, risk assessments, policies, controls and staff training. The fine was announced following a separate HMRC, Metropolitan Police and FCA month-long crackdown on MSBs suspected of being used for money laundering.

2.30 This highlights the pro-active approach HMRC is now taking to tackle money laundering and regulatory non-compliance and the potential public penalties possibly imposed.

8

External Threats: the Banking Framework and Operation Admiralty

2.31 The number of high value and complex cases relating to banking deposits continues to increase:

- Between 1st July and 27th October 2019 there were 25 investigations relating to partner banks (12 during September/October); the total amount linked to these cases is c.£16m.
- This is in comparison to 16 cases during the same period in 2018. Post Office is taking all reasonable actions to identify these transactions (which are anonymous to us) and raising SARs with the partner banks and law enforcement.

2.32 As a result of recent banking deposit cases, the Financial Crime team, together with two Network Area Managers, Security Operations and the NFSP visited 52 East London branches on 25th October 2019 to raise awareness of criminal activity and the importance of raising SARs. The visits were well received and key learnings will be reviewed to inform further training and awareness across the network on AML issues.

2.33 The National Economic Crime Centre (NECC) and the Pro-Active Taskforce at the Economic Crime Directorate (attached to the National Crime Agency), approached our MLRO to help them understand and tackle the migration of

POL00423684

placement risks from banks to Post Office. As a result the NECC has established Operation Admiralty, with participation from Post Office, Lloyds, Barclays, RBS, HSBC, Santander, HMRC and the NCA. The first meeting took place on 23rd October 2019 with all key stakeholders in attendance, and a follow-up meeting is planned for 6th December 2019.

External Threats: Gambling Commission fines

2.34 The Gambling Commission has applied sizeable fines on firms such as BetFred, Ladbrokes Coral and others in part for failings in respect of vulnerable customers and AML practices.

2.35 We are concluding the risk assessment of sales of The National Lottery and scratch cards in Post Office branches. Currently there are no limits on the number of games a customer can purchase, and no guidelines issued to staff in relation to vulnerable customers. The draft report will include a recommendation for the product manager to review with Camelot what controls can be put in place to address the issues around vulnerable customers raised by the Gambling Commission. Losses in relation to reconciliation and activated unsold scratch cards have been highlighted to the Product Manager (also see Supply Chain Compliance below).

Supply Chain Compliance

2.36 Four site audits were completed between September and October 2019 with 18 Improvement Needs identified. Whilst this is higher than we have seen at recent audits, it is on par with Improvement Needs identified at these sites previously. However we are monitoring to ensure that we do not see the same issues at other sites.

- There was one low risk recurring issue identified at Norwich relating to documenting 121s
- Two key issues were identified during the London audit – the interim control to oversee a flaw in CWC outward remittance functionality (which allows clerks to re-print their own barcodes) failed and £2k was found in the vault that was not accounted for; this is under investigation
- The remaining 15 related to minor issues, mostly documentation issues.

2.37 One supplier audit on HR was conducted with 2 Improvement Needs identified.

2.38 The NSI conducted an external audit of Aberdeen and Glasgow which found no reportable improvement needs and highlighted four observations.

2.39 The compliance team is conducting an end-to-end review of Supply Chain value stock processes (which includes scratch cards, stamps and phone cards) and have identified a number of control gaps. The team are engaging with the Head of Loss Prevention and Internal Audit to ensure that a complete picture of supply chain risks is understood. The draft report on findings is expected to be completed during Q3.

8

Financial Services

Credit Cards

2.40 Following the agreement with Capital One to provide credit cards the Regulatory Guidance Manual (which sets out the ways of working for compliance) has been agreed with our new regulatory Principal. This is broadly aligned with how we work with BoI and POI.

2.41 Customers can apply for a Capital One Credit Card through the Post Office website as digital marketing began on 4th November. We are also working with Capital One on how a pilot for branch distribution, initially as lead capture, could work compliantly.

Mystery Shopping Results

2.42 Mystery Shopping results continue to be mixed, with further improvements in Savings but on-going poor conformance in Travel Insurance and Life.

- Savings – no reds in October and only 1 in the 3 months up to October.
- Travel Insurance – too often colleagues are not sharing the Eligibility and Medical Conditions laminate with customers so that customers can confirm their medical condition status
  - The first phase of changes to the Travel Insurance journey have gone live on 4th November, the 2nd phase is due to go live mid-March.
- Life Insurance – 2 reds were recorded for failing to follow the onscreen instructions for the Easy Life journey. In the 3 months to October we recorded 16% reds. Further discussions have taken place with POI Compliance to push through the requested changes to the system and questions with the product teams.

2.43 Remedial activity:

- A Sales Quality Improvement Group has been set up between Post Office Insurance and Post Office. The group consists of product managers, compliance teams from POI and POL, training and representatives from the Network field teams. The group's purpose is to work together to understand areas of weakness and agree actions to improve the quality of POI sales
- Medical screening details will be included in the product literature from March 2020, removing the need for the separate laminate.
- The Insurance Compliance training module is being developed to include the introduction of 3 levels of cover (due to go live in March 2020) and will include automated processing through Horizon;
- Face-to-face training for Area Managers is being planned in Q4 to help them support branches with the revised process;
- Production of a training video, which will be distributed to Area Managers to share with branches;
- Quarterly Capability Events – Each region will be running some smaller events within geographical areas to grow the capability of branches where we feel a risk has been or could be identified. Focus will be across all FS products where the agenda will be shaped according to latest results/trends.

CRM support structure

2.44 The CRM support structure is now in place with 4 Area Managers performing the role of Support Manager. POL Conduct Compliance is monitoring performance and providing support and guidance. Gaps in activity are being closed with plans in place to close all gaps by mid-November. CRMs are experiencing problems with the browser on the Tablet which is causing Tablets to malfunction. IT is supporting network to find a solution. This issue is impacting CRMs ability to help customers.

Vulnerable Customers

2.45 This is a key regulatory theme across government and regulators. Ofcom issued a consultation 'Treating Vulnerable Customers Fairly' with a closure date this November. Ofcom expect senior level proactive engagement to ensure vulnerable customers are treated fairly. The Telco team are broadly supportive of the consultation but will feedback some operational and data protection points to the regulator.

2.46 Similarly FCA issued a draft guidance paper in July focused on the fair treatment of vulnerable customers. This focuses on the skills and capabilities of staff to

support vulnerable customers, how customer processes react to the vulnerability challenge and how firms monitor how well they perform.

2.47 We will be reviewing and reporting on our Post Office wide initiatives at the Vulnerable Customer Action Group on 14 November.

Regulatory Diary

2.48 The FS Regulatory Diary is included in the supplementary information as Appendix 7.

Supplementary information

2.49 The following supplementary information has not been specifically referenced in this report, but is available in the reading room:

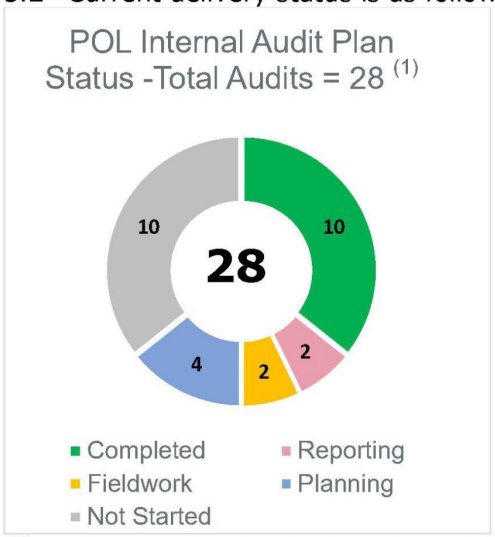
- Compliance dashboard (Appendix 8)

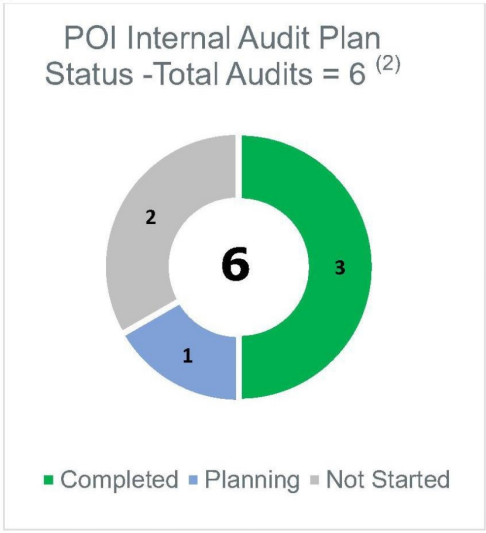
3. Internal Audit — Author: Johann Appel

Progress against plan:

3.1 Delivery of the 2019/20 programme is making good progress, having finalised eleven audits since the September ARC meeting (9 POL and 2 POI).

3.2 Current delivery status is as follows:





(1) POL ARC approved baseline plan for 2019/20 (18 core internal control reviews & 10 change assurance reviews). Details of the audit plan status are included in the reading room (Appendix 9).

(2) POI ARC approved baseline plan for 2019/20 (5 internal control reviews & 1 change assurance review).

Internal Audit reviews in progress and planned

3.3 The following reviews are in progress or being planned for delivery in Q3:

	Review	Status	Timing
Post Office Ltd			
1	PCI Compliance Programme (Change)	Reporting	07/10 - 01/11
2	CFS Controls	Fieldwork	14/10 - 15/11
3	Telco Billing Process	Fieldwork	04/11 - 25/11
4	Cyber Security Follow-up	Reporting	28/10 - 29/11
5	Branch Banking Framework	Planning	02/12 - 20/12
6	HIH (Change)	Planning	25/11 - 13/12
7	Accounts Receivable	Planning	06/01 - 24/01
Post Office Insurance			
8	Oversight of Third Parties	Planning	Dec

POL00423684

Internal Audit reviews completed

3.4 Since the September ARC meeting we have finalised the following 11 reviews:

1	Employee Expenses Follow-up		7	Effectiveness of 2nd line Programme Assurance (Change)	
2	Purchase to Pay		8	SGEI Validation	
3	Payzone Control Framework		9	Archer Implementation (Advisory)	
4	Data Analytics and Excellence (Change)		10	Nemesis Programme Assurance (POI)	
5	Effectiveness of the Gating Process (Change) [1]		11	Change Capacity (POI)	
6	Benefits Realisation (Change) [1]				

[1] Benefits Realisation and Gating Process were combined into a single report.

3.5 Our findings and observations from the POL and PZBP reviews are summarised below, with the full reports available in the reading room.

Employee Expenses Follow-up (Ref. 2019/20-03)



Sponsor: *Lisa Cherry*

Audit actions:

P1	0
P2	10
P3	1
Total	11

The 2018/19 audit was rated RED (unacceptable) due to the poor control environment that existed at that time. There were gaps and inconsistencies in the level of control exercised by line managers, with a significant issues around both the quality of receipts (where presented) and the lack of receipts (in a large number of instances).

This follow-up audit has found that the control environment around employee expenses is much improved. Considerable remedial work has been undertaken by the business to improve controls over employee expenses, with a new Travel and Expenses Policy produced and communicated to the business in January 2019. The business took this opportunity to acknowledge challenges from the field teams and made improvements to ensure the policy more fairly reflected their needs as well as those of the frequent business traveler.

The amount of expense claims without receipts have improved from 8.8% to 1.8%. Corporate Procurement Cards have been further reduced from 35 to 25, the provider has been changed and the controls strengthened, including the requirement for receipts to be provided and authorised by the card holder's line manager via the Selenity system.

The areas of reward and recognition and HMRC rules around benefits in kind still need to be fully addressed and there is a need to further improve the provision of supporting receipts for both expenses and Corporate Procurement Card (CPC) spend.

Management Comment provided by Lisa Cherry

The findings of the audit compared to the previous expenses audit in 2018 are a marked improvement and encouraging to see the collaboration that has taken place has improved the governance around expenses. Thank you to the Audit Team for their support throughout this piece of work. However, it is important to note that there is more work for us to do collectively around the taxation rules and treatment of expenses, policy ownership and the key contributors/stakeholders to the overall expenses processes. Identifying and agreeing roles and responsibilities across POL is key for a compliant and effective policy combined with supporting processes to further aid the appropriate governance, framework and operational rigour required.

8

POL00423684

Purchase to Pay (Ref. 2019/20-02)



Sponsor: *Al Cameron*

Audit actions:

P1	0
P2	6
P3	0
Total	6

We conclude that controls over P2P are mostly effective, despite the inherent limitations of the outdated system. The current P2P system is very manual, not user friendly and has limited capability to provide meaningful management information, which impacts decision making. Purchasing decisions are not as smart as they could be as there is no link to supplier contract terms (e.g. minimum order quantities, pricing and applicable discounts), spend to date detail or cost centre budgets.
Performance against the 30 day payment regulations is currently at 99%. Use of 'one time' vendors has been significantly reduced, although we found that one time vendor accounts are not consistently blocked after use. The audit identified control weaknesses around user access and vendor master data, which are easily resolved.

Management Comment

Both Procurement and Finance teams put considerable effort into maintaining good controls around Post Office spend management. They do a very good job given that they rely heavily on manual controls with a system which is overdue for upgrade and enhancement to reflect more modern practices, automated controls and transparency. However, we recognise that there is always room for improvement and the actions assigned from the audit will be actioned immediately. *(Michael Passmore – Finance Director; Barbara Brannon – Procurement Director)*

Phase 2 of the Source to Settle Project was approved by Investment Committee on 24 September. Well done to all the teams maintaining controls in a very sub-optimal environment. *(Al Cameron – CFO)*

8

Payzone Control Environment (Ref. 2019/20-04)



Sponsor:
Debbie Smith

Audit actions:

P1	1
P2	10
P3	4
Total	15

Post Office acquired Payzone Bill Payments Limited (PZBP) on 19 October 2019. With this acquisition, Post Office gained an additional network of approximately 13,000 bill payment outlets, along with Payzone's bill payment technology and 74 staff. An internal audit of the Day1-100 programme to integrate PZBP was completed in May 2019.
This review of the control environment at Payzone was requested as part of the 2019/20 IA plan, approved by the ARC. This review aimed to assess the appropriateness of Payzone's control environment considering the nature, size, and key risks of the business. This was a high level controls 'health check' of key controls across the organisation.
We conclude that the control environment within the Finance and IT functions of PZBP is mostly sound and fit for purpose for an organisation of PZBP's size and complexity. The completion of full separation from the previous owners PZUK remains on track. Where segregation has yet to be achieved TSAs are in place across both Finance and IT key functions. A Separation Programme is in place to track required actions. PZBP continue to work to remediate issues identified during PO sponsored independent security testing and to integrate data protection processes.

Management Comment provided by Andrew Goddard

A significant amount of work and improvements have been achieved in the first year to separate the two companies. Whilst some things remain to be done in the separation, it is pleasing to note that the control environment is in a good state to give confidence in our daily business. We are working on further improvements to incorporate the recommendations in the report and are committed to deliver them by the due dates.

POL-BSFF-0238502_0073

POL00423684

Data and Analytics Excellence (Programme Assurance) (Ref. 2019/20-05)



Needs Significant Improvement

Sponsor:
Shikha Hornsey

Audit actions:

P1	0
P2	10
P3	1
Total	11

The Data and Analytics Excellence (DAE) programme, previously called Arrow, was approved at CAG in February 2018 with the aim of enabling the use of information as an asset for Post Office. Prior to this Post Office lacked data governance, data policies, procedures and standards for data, which had resulted in multiple versions of 'core' data to which users had access to depending on their location, function, and data provider. There was a general perception that this was impacting the reliability of data across Post Office.

The objective of this review was to assess the extent of the programme's delivery to date, highlighting key observations on the programme and practical considerations for the programme to take into account as it transitions its work into operations. Specifically we assessed controls over:

- Project initiation and delivery; and
- Project closure and transition to the revised delivery model.

We conclude that the DAE programme partially delivered against its objectives (as revised from the original business case), with some successes noted. However, we have identified control failings at all levels of programme governance and delivery, most significantly:

- The programme has not received formal approval for the entirety of its business case scope and deliverables;
- The target maturity level for Data Governance and Data Management was not defined upfront, which reduced the programme's ability to outline and measure the value contribution and key deliverables of each phase;
- The programme delivery was adversely impacted by insufficient committed resources and competing priorities.

Whilst the programme has now closed, we highlight the need for lessons to be learnt (in particular for the benefit of the ongoing programme to decommission Credence) and for improved governance over the transition of the programme to BAU.

8

Management Comment provided by Al Cameron

While we have made some progress in improving operational MI, data governance, and got clarity on the core system changes needed, this is not a good read. In spite of joined up executive sponsorship, the project was be-devilled by two issues which took a long time to resolve and longer than they should.

The relationships between IT – and particularly the architecture team at the time – and the data team consistently failed to operate successfully in spite of repeated interventions. We sought to resolve this by bringing it all within the CIO's ownership but this led to the data team being substantially dismantled and ceasing progress.

In addition, a similar and problematic relationship developed between the data team and the change governance processes so that the business case was endlessly recycled and re-written – and therefore not formally approved – without anyone wanting to cease what was valued and important work.

Separating the change governance from IT and bringing in Dan Zinner as CTO is helping materially and with the change in the architecture team these problems will not recur. The fundamental issue – how do we make the progress on MI and data that the business so desperately needs – is firmly on the PSG agenda but is today unresolved including leadership within the data team which may have been a contributing factor.

POL00423684

Effectiveness of Gating Process and Benefit Management (Ref. 2019/20-07)



Sponsor:
Dan Zinner

Audit actions:

P1	0
P2	4
P3	1
Total	5

This report combined the findings from two distinct audits to assess the effectiveness of: 1) the Gating Process; and 2) Benefit Management (Product Realisation). These are two key areas where weaknesses were highlighted in previous internal audit reviews and lessons learnt from project delivery. Both reviews assessed only the design of the controls against the recently introduced Change Excellence Framework (CEF), the revised change methodology, which replaced One Best Way (OBW).
We have found that the revised controls over Gating are generally well designed and the enhancements done in the Benefits Management space will drive greater transparency and rigor to the processes, thus addressing the shortcoming noted in past audit reviews. However, we highlight that the revised change methodology (CEF) is in its early stages of adoption and as such will require time to bed in. This includes training the Change community and transitioning of in-flight projects. CEF implementation is also being done alongside significant organisational changes, including re-defining the portfolios, roles and reporting lines, thus adding complexity and a period where control weaknesses may persist. While this work is ongoing and we have seen positive impact, particularly in greater clarity over responsibilities for project delivery, we highlight key areas of focus that will improve the controls over Gating and management of Benefits.

Management Comment provided by Dan Zinner
We found this audit to be helpful in pointing out areas where we can improve our governance process. There is always room for improvement, and thus seek clarity on specific areas from IA and an understanding of prioritisation based on IA findings so we can focus our efforts.

8

Effectiveness of the Second Line Change Assurance (Ref. 2019/20-09)



Sponsor: *Dan Zinner*
Audit actions:

P1	0
P2	4
P3	0
Total	4

The objective of this review was to assess the design effectiveness of the Second Line Change Assurance's governance, processes and controls. The audit has identified opportunities to improve the Second Line Change Assurance activity by consolidating into a single plan and optimising the assurance provided by the CRA team with the pockets of assurance introduced by the SPO as well as new controls being implemented as part of the Change Excellence Programme. The review also highlighted that there is a need for greater clarity over the forms of assurance and the roles and responsibilities of the second line. We highlight that certain controls (such as gate approvals) will now be operated by the SPO and as such care should be taken to have sufficient segregation of activities within the SPO to allow for the second line activity to operate impartially.
We are aware that the Change organisation and processes are currently under review and that the recommendations from our audit will be considered as part of this process. Internal Audit will perform a follow-up review to assess the effective operation of the revised control environment in due course (scheduled for Q4-2019/20).

Management Comment provided by Dan Zinner
We found this audit very useful and aligned to many of the initial observations the CTO had when starting at POL. These are aligned with the ARC paper the CTO outlined, but has gone further to highlight some of the issues around control and assurance. As such the CTO welcomes IA's report and requests additional support from IA in the form of workshops and frameworks that the various stakeholders in Change can use to create the detail around the recommendations in this report.

POL00423684

SGEI Validation (Ref. 2019/20-12)	
 Needs Improvement ***Sponsor:*** *Debbie Smith* Audit actions: P1: 0 P2: 4 P3: 0 Total: 4	This review assessed the governance, oversight and process around POL's compliance with its SGEI obligations. Additional work was undertaken to validate the reported SGEI position relating to the 2019 Network Report (as at March 2019). Work undertaken by Internal Audit indicates that the SGEI position reported for March 2019 accurately reflects POL's SGEI delivery and that the reported position satisfies the common understanding of SGEI provision requirements in the Funding Agreement. The review highlighted the need for action to clarify elements of the requirement and the process by which it is managed. In particular: • Agree changes to Annex A services (of the Entrustment Letter) with UKGI; • Review SGEI products against Annex A categories to ensure that all and only SGEI products are reported; • Establish the level of assurance needed to verify the availability of SGEI products; and • Strengthen end-to-end oversight through clear ownership.
Management Comment provided by Tracy Marshall We are pleased that this review found that POL continues to deliver its SGEI obligations. The agreed actions will add clarity to the requirements and facilitate the effective ongoing monitoring and reporting of SGEI products.	

Archer Implementation (Health check) (Ref. 2019/20-14) (Advisory Review)
The Central Risk team seeks to leverage the existing RSA Archer GRC tool to enhance the effectiveness of risk management in Post Office. Phase 1 of the implementation of the Risk Management 'use case' aimed to deliver an Archer solution which allows Post Office to migrate their 50+ spreadsheets of risk registers across the business into the GRC tool. This was an advisory review to confirm that the build of phase 1 of the Archer risk tool was appropriate and would not restrict any future enhancements and developments. Deloitte concluded that based on the documentation received and Archer configuration reviewed, the primary business objective of the phase 1 solution should be achievable, provided that the data meets the required level of quality for successful migration. The business accepts this and the Central Risk team are currently working with the business to review and refresh risk before they are migrated to Archer. Additionally the Central Risk team accepted that it would be prudent to work with the other business areas already utilising (CISO) or considering using Archer (Finance and IT) to create a governance body to develop a strategy or framework and manage GRC changes and processes. The Head of Risk will lead on the creation of this and will look to have this in place by January 2020. The review also provides some recommendations for the future development of the GRC tool, which will be considered during phase 2 (subject to a further business case and benefits analysis).
Management Comment provided by Mark Baldock I acknowledge the findings of the Advisory review and agree Archer Phase 1 implementation (Central Risk system live and all business risks cleansed and loaded) is broadly achievable in the timeline. There are a small number of UAT defects provided to the supplier for resolution. Analysis suggests these are of relatively low priority. Phase 1 implementation requires provision of a standard Post Office organisational hierarchy against which business risk ownership can be allocated. This is not yet available and is likely to be subject to the outcome of the CEO's 100 day plan. A clear project dependency but workaround being explored. Wider rollout to business community requires a stable service wrap (to cover standard queries, password resets etc). This is not yet in place and a route to green not yet agreed. We are drafting formal Go/No-Go criteria to underpin the Archer Phase 1 implementation decision. Central Risk will put in place a scaled Archer governance structure by end 1/2019.

8

POL00423684

3.6 Following are summaries of the two POI audits that were finalised and presented to the POI ARC:

Nemesis Programme Assurance (follow-up)	
 Needs Improvement ***Sponsor:*** *Ed Dutton* Audit actions: P1: 1 P2: 5 P3: 0 Total: 6	Internal Audit conducted a review of the operating effectiveness of delivery activities, including project oversight and go/no-go governance, system integration testing, user acceptance testing (UAT) and business readiness. The report was rated 'Needs Improvement'. Overall, programme management and governance was effective, with POI leadership being sufficiently aware of the key risks and issues impacting the programme for an informed go/no-go decision at the go-live gate. Ultimately the decision was made to postpone go-live to 8th October, until the completion of key deliverables. In addition to noting that a significant number of key deliverables was pending completion and sign-off at the time of the audit, IA noted some deficiencies during fieldwork that were remediated by management prior to go-live. These include some UAT defects that had not been appropriately logged and addressed. Other findings that were not Day 1 critical will be incorporated in subsequent Nemesis releases as well as providing lessons learned for future programmes. These include timely agreement of each go-live criteria and clear cut-off for change requests.
Management Comment provided by Michelle Downs The audit activity was requested by Change to support successful delivery of the programme and to confirm business readiness. During the scoping of this audit phase it was specially requested to focus on business readiness in the contact centre and supporting functions. The audit scope did include the wider readiness activity, however the report focuses more on more traditional project governance. Of the 7 actions identified 3 were already being addressed and complete ahead of the report the remaining 4 are in progress.	

Change Capacity	
 Needs Improvement ***Sponsor:*** *Ed Dutton* Audit actions: P1: 0 P2: 3 P3: 0 Total: 3	This review looked at change activity underway across POI and assessed the design and operating effectiveness of the processes and controls in place to manage delivery, focusing on capacity planning. Overall we found that POI is continuing to deliver its planned change programme and has visibility over activities that are managed by the Change Team. However, there is no reported consolidated position that includes change being delivered outside of the Change Team. Although these are typically smaller and less complex in nature, without visibility of all change activities POI is unable to assess the impact of its overall commitments, including interdependencies, accurately. We also noted that there is a lack of clarity around the process for business change management, particularly around the mechanism by which change is identified. As a result, it is likely that not all change has been identified. Additional observations were made around the impact of a key vacancy within the risk team and the dependency on POL to deliver elements of change. An overall rating of 'Needs Improvement' was given.
Management Comment provided by Ed Dutton POI is entering the final stages of a significant transformation, and its fundamental strategic approach in the short term is to focus on driving value from the previous investments in an environment of significantly less change. Part of that effective execution approach includes senior teamwork and effective governance, communication and controls, and management are supportive of refreshing these to enable effective delivery of their plans in a more stable environment.	

8

POL00423684

Status of Audit Actions:

3.7 Audit actions are generally being completed on time. Since the September ARC, 31 actions were completed and 56 new actions were added. As at 15 November 2019 there were 75 open actions, none of which were overdue.

Audit Action Status (POL):	
Open (not yet due)	75
Overdue (<60 days)	0
Overdue (>60 days)	0
Total	75

Review of the current year audit plan:

3.8 In line with the Post Office Internal Audit methodology, we performed a mid-year review of the 2019/20 plan to validate that the plan is still aligned with Post Office's risk profile and that the remaining audits on the plan are still relevant.

3.9 Following discussions with senior management, it is our view that the number and focus of the reviews on plan are still appropriate and we recommend only one change at this time:

- To postpone the audit of Branch Cash Forecasting to 2020/21 to allow for the current re-engineering of the process to be completed and new controls to be embedded.

3.10 The total number of audits on plan will remain unchanged following the addition of the SGEI review earlier this year. The amended plan is included in the reading room as appendix 9.

3.11 The programme assurance reviews on plan (currently 10) are being assessed on an ongoing basis to reflect the programmes most deserving of independent assurance, predominantly 'Platinum and Gold' projects. The list will be reviewed and updated following the 'funding pause' and re-prioritisation of the Change funding spend, which is currently undertaken by the Investment Committee.

END OF REPORT

8

POL00423684

Policy Summary Paper

Author: Paul Beaumont Sponsor: Jonathan Hill Meeting date: 25 November 2019

Executive Summary

Context

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

Questions addressed in this paper?

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

Conclusion

In order for Post Office to maintain its policy governance responsibilities, owners need to review their policies regularly.

Input Sought

The Committee is asked to review and approve the updated policies

9

The Report

Which policies were updated in this annual cycle review?

In this review cycle 3 policies were revised pending approval.

Policy	Last Reviewed	Updates
Risk Policy	June 2013	See separate ARC paper
Change Management Policy	July 2017	Refresh
Personal Data Protection	October 2018	Refresh

What updates were included and why?

A summary that identifies the changes and updates that has been included has been added below:

Change Management Policy

Strictly Confidential

POL00423684

- Removal of Post Office Insurance from the Post Office Group Change Management Policy.
- Change of policy sponsorship and ownership, noting Dan Zinner as Chief Transformation Officer under both roles.
- Risk appetite statement updated to reflect the current tolerance levels, specifically calling out the response to legal and regulatory responsibilities, including litigation, commercial practice and financial crime.
- Inclusion of minimum control standards, specifically outlining the controls and processes in place to minimise the identified risk throughout the delivery of change.

Personal Data Protection Policy

- The Protecting Personal Data Policy has been amended to ensure it reflects industry best practice and provides clarity in relation to Post Office processes and policy in relation to the management of personal data, reduction of data protection risk and compliance with Data Protection legislation.
- There have been no legislation changes in the past year however there has been considerable development in best practice and case law.
- Minor amends have been made in relation to:
    - Clarification of controls
    - New minimum control
    - New section relating to processing of Special Category Personal Data for employment purposes and travel insurance

Policy reflects improved processes relating to Documents and Records management and use of OneTrust system.

ENDS

Strictly Confidential

POL00423684

POST OFFICE LIMITED
AUDIT RISK AND COMPLIANCE COMMITTEE

Risk Policy Review

Author: J Ellwood Sponsor: Al Cameron Meeting date: 25 November 2019

Executive Summary

Context

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

Questions this paper addresses

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

Conclusion

- The Risk Policy has been transferred into the new Post office standard template and restated to ensure it reflects industry best practice. It provides clarity on governance arrangements through the articulation of core principles, expanded risk universe categories, and updated roles and responsibilities, as well as inclusion of minimum control standards.
- In parallel, work has been undertaken to review and refresh the Risk Management Framework (RMF). A single document has been developed to reflect current processes and supports the Policy. This document is available to members in the reading room. An intranet site is also now available which makes all risk information more visible to the business.

10

Input Sought

The ARC is asked to review and approve the updated Risk Policy.

POL00423684

The Report

Why do we need to review this Policy?

1.1 The Policy was last reviewed and approved by the ARC in October 2014. The terms of the Policy will be considered annually going forward.

What changes to the Policy do we propose and why?

1.2 The existing Policy has been translated into the new Post Office standard template and enhanced, updated with additional sections drafted including: core principles, application, roles and responsibilities, reference to key Risk Management processes and related supporting policies.

1.3 Ways of working have also been more formally articulated which include:
- Referencing the Risk Management Framework (RMF) which sets out the approach for the identification and management of risk within the Group
- Significant incident reporting, risk exception and appetite processes
- Minimum control standards to manage risks

What are the implications of these changes?

1.4 Whilst no material changes are required to comply with this updated Policy, implementation of the Archer GRC tool, will inevitably result in more automated processes driving activities and tasks e.g. risk recording and assessment.

1.5 This Policy will also support the delegation and embedding 1st line responsibilities.

10

What would be the impact be of delaying approval?

1.5 The Policy is the highest level document to set out our risk approach at Post Office. It provides our strategic vision and articulates what our risk and control environment should look like. Furthermore regulators, auditors and some third parties, view it to be an essential operating tool and expect to review them as standard practice.

POL00423684

Pension Scheme Controls

Author: Maxine Cross Sponsor: Al Cameron Meeting date: 25 November 2019

Executive Summary

Context

This paper sets out the current controls in place to manage our company pension scheme and whether there have been any changes in controls since last year.

Questions addressed in this report

1. What are the controls in place for our current pension scheme?
2. Have there been any changes in controls since last year,
3. Whether there had been any significant control breaches or changes since.
4. What are the ongoing activities in relation to our pension scheme?

Conclusions

1. The current pension scheme is the Scottish Widows Group Personal Pension plan and is controlled in a number of ways. The key controls include written procedures and documentation, the ongoing processing controls which exist in HRSC and the Pensions Governance Committee
2. The key changes in controls that have occurred since 2018 include; the additional procedures and documentation that has been established following completion of the actions from the 2018 red audit and the June 2019 green audit. In addition there is much stronger collaboration between Reward, HRSC, Audit and the risk teams. The format of the Pensions Governance committee has improved in its organisation and content following the change in key resources within the Post Office Reward team. Furthermore there is now a documented annual and long term reward plan which includes pensions and this plan is monitored and tracked to identify any key pension activities.
3. There have been no further breaches recorded since the recent June 2019 Audit.
4. There are ongoing activities in relation to our pension scheme which will further mitigate the associated risks with the scheme which include a planned risk workshop with the Reward team. This will be led by the risk team to carry out a full risk review of all Post Office benefits. There is also ongoing continuous improvement activity in relation to the Governance committee, which a fully minuted and tracked, examples of this include improvements to the quartley governance report and the development of an ongoing issues log of any process / SLA issues that require reporting, action or escalation.

Strictly Confidential

POL00423684

Input Sought

1. ARC is asked to note the current position.
2. ARC is asked to note the ongoing activities

Input Received

1. Reward

POL00423684

UK Data Protection Act (incorporating GDPR) Compliance Status Report

Author: Jonathan Hill & Chris Russell Sponsor: Ben Foat Meeting date: 25th November 2019

Executive Summary

Context

1. This paper is supplementary to the UK Data Protection Act (incorporating GDPR) Compliance Status Report presented to July 29th ARC. The July paper is attached in Appendix A (in the Reading Room).
2. The General Data Protection Regulation ("GDPR") was a re-alignment of the balance of power between organisations and individuals. Whilst organisations needed to use personal data for commercial purposes there were concerns that individuals, customers and employees, had lost control over their personal data. The purpose of the GDPR was to address that balance and give power back to the individual. GDPR is incorporated within the Data Protection Act 2018 (DPA).
3. Further to the paper presented in July, GE members have asked for an update on the status of Post Office compliance, with particular reference to the contract remediation work being carried out.
4. This paper provides the Compliance assessment of Post Office's conformance with the DPA and an update on the actions being taken. This does not include Payzone, which is subject to a separate review on data protection, currently underway.
5. The Committee is asked to note the update.

Questions this paper addresses

- What are the GDPR requirements?
- What activities has Post Office undertaken to date to comply with the DPA?
- What further actions are needed to ensure that Post Office achieves and sustains the required level of compliance?

12

Conclusion

1. In consultation with peers from other organisations, Post Office position is on a par with most major firms and ahead of many.
2. Post Office has reported through to the ICO numerous incidents and breaches that have occurred since GDPR was introduced and in all instances the regulator has found in favour of the actions we have taken with no sanctions applied.

POL00423684

3. All customer complaints that have been reported to the ICO have been managed effectively by Post Office with no further action taken against any complaint raised to date.
4. There are areas where we can never state that we are 100% compliant. However, when a new issue is identified, we have the processes in place to expedite remediation.
5. We will continue to develop our Privacy Maturity Framework to ensure that we can report with confidence on our levels of compliance.
6. The Remediation work is expected to be completed by the end of June 2020.

Input Sought

The Committee is asked to note the Compliance update.

POL00423684

Report

What are the GDPR requirements?

1. The legislation dictates:
   - 1.1. Greater transparency regarding the use of data;
   - 1.2. Enhanced individual rights including higher thresholds for consent to be legitimate;
   - 1.3. Obligation for data controllers to make it easier for individuals to access their own personal data;
   - 1.4. Greater flexibility in the portability from one data controller to another,
   - 1.5. Increased controls by a data controller when personal data was shared with other organisations; and
   - 1.6. Introducing the concept of Privacy by Design.

2. Other administrative requirements include:
   - 2.1. Ensuring that contracts between organisations set out clearly where the responsibility for data handling lies;
   - 2.2. Due diligence obligations on new and existing service providers were enhanced; and
   - 2.3. Records of processing activities were created and maintained.

What activities has Post Office undertaken to date to comply with the DPA?

3. In common with virtually all data controllers and processors, Post Office's initial gap analysis highlighted significant deficiencies in Post Office compliance with the DPA. Given the size and complexity of data processing this was not unexpected. The legislation, being principle based, allowed a degree of flexibility on implementation. Post Office, in line with many other organisations adopted a risk based approach with two defined phases for implementation.
   a. Phase 1 – use of customer data in Post Office ("effective" compliance)
   b. Phase 2 – updating administrative processes and controls ("substantive" compliance)

4. Phase 1 focussed on enabling Post Office and Post Office Insurance to continue to operate as before but updating the way in which customer data was collected, stored and used. Changes included:
   - 4.1. The way customer personal data was collected specifically for marketing purposes;
   - 4.2. New rules and protocols were introduced into the Brands database to allow the optimum use of customer records;
   - 4.3. Streamlined processes allowing greater control by individuals over their data including access to information and right to be forgotten were implemented;

POL00423684

4.4. All internal and external privacy policies were re-written to ensure compliance but still allowing the organisation to maximise the commercial use of customer data.

5. Phase 1 delivered on its key objectives and these processes continue to be assessed and monitored for ongoing compliance.

6. An independent audit of Post Office's approach and implementation of Phase 1 was conducted by PWC which reported favourably on both with no significant failings.

7. Phase 2, initially running in parallel with Phase 1, focussed on delivering the administrative elements of the GDPR. This was predominantly around demonstrating Governance and Accountability where evidence of compliance was formalised. This included such evidence as Records of Processing, Incident Management procedures and Privacy by Design, (including Data Protection Impact assessments). Training was created and delivered across Post Office.

8. Critically, Phase 2 included remediating Post Office contracts. Given the scale and complexity of the contractual landscape, external Legal support was engaged to manage and run this remediation on Post Office's behalf.

9. The remediation process faced a number of challenges including having a number of third parties who failed to engage. There remain 33 that have not responded to date.

10. Towards the end of Phase 2 an additional 159 contracts were discovered by Procurement, though the majority of these are low risk IT Licence agreements or low risk contracts. These contracts were not included in the original GDPR programme, however they are now included in the remediation plan.

What further actions are needed to ensure that Post Office achieves and sustains the required level of compliance?

11. The GDPR programme was closed in April 2019 with two deliverables not completed:

    11.1. Contract Remediation; and

    11.2. The measurement and demonstration of on-going Compliance.

12. In the interim period Compliance and Legal have been working their way through the outstanding contracts, prioritising those that were due for renewal or where the contracting party pushed for completion.

13. Excluding the additional 159 contracts referenced above, which are expected to be low level risk, there are 84 original contracts requiring remediation of which 12 (see Appendix B) are deemed to be of high risk: often the issue is that GDPR remediation is only part of wider contract negotiations.

14. For each of the material contracts we have reviewed our activity plans and are prioritising those deemed the highest risk. We have a project team in place and will work alongside the contract owners to drive engagement and resolution.

15. As proposed in July, a more robust approach is being adopted with regards to the non-material contracts where we have made at least two attempts to contact Service providers. A third remediation pack will be sent including a letter where unless a response is received we will 'deem consent'.

POL00423684

15.1. Deemed consent will not remove the legal risk but is a pragmatic approach to close out the remediation work.

15.2. 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.

16. Regular project reporting will ensure that we are on track to deliver and can highlight where additional support may be needed.

17. On-going compliance is being developed with the Privacy Maturity Framework driving that process (please refer to the July ARC paper in Appendix A). All the correct evidence gathering methodologies are developed and being managed. The key focus now is on ensuring this forms part of the business as usual behaviours within the business.

18. We are focusing on remediating all of the outstanding contracts by end June 2020.

Conclusion

19. Set out in the July 2019 paper to the ARC are the Privacy Maturity Framework metrics. We are confident that these accurately reflect the current position.

20. In consultation with peers from other organisations, Post Office's position is on a par with most major firms and ahead of many.

21. Post Office has reported through to the ICO numerous incidents and breaches that have occurred since GDPR was introduced and in all instances the regulator has found in favour of the actions we have taken with no sanctions applied[1].

21.1. For example, the ICO backed our approach to Breach Management in response to the recent "MBA" incident by taking no further action and backing the remediation plan we applied.

22. All customer complaints that have been reported to the ICO have been managed effectively by Post Office with no further action taken against any complaint raised to date.

23. There are areas where we can never state that we are 100% compliant. However, when a new issue is identified, we have the processes in place to expedite remediation.

24. We will continue to develop our Privacy Maturity Framework to ensure that we can report with confidence on our levels of compliance.

25. The Remediation work is expected to be completed by the end of June 2020.

[1] The Fixed Penalty Notices Applied are under Privacy and Electronic Communications Regulation for late notice of an incident.

POL00423684

Appendix A – July 2020 ARC GDPR status update

POL00423684

Appendix B – Outstanding GDPR high risk contracts

Party	Contract Matter	Current status
Fujitsu	[redacted]	
OH Assist	Provision of occupational health and wellbeing services to Post Office	**Under Review/Negotiation** OH Assist challenging their position as a Data Controller.
Experian	Security Vetting	**Under Review/Negotiation** POL reviewing Experian's contract clauses as they are insistent we use theirs.
SAP UK Limited	MYSAP Software License & Maintenance Agreement	**Investigation** POL checking new contract that was signed recently to ensure GDPR compliance
Computacenter	End User computing (provision of equipment & support/maintenance)	**Under Review** POL IT considering future relationship with CC, contract to be remediated if current position is extended.
RAPP	Data Analysis, Direct Mail, Email & SMS	**Investigation** POL decision on extending RAPP contract or procuring new provider required prior to remediation
Gemalto	IT support for Application, Enrolment and Identity Services	**Under review** POL reviewing Gemalto's contractual clauses
Fujitsu Telecoms	Telecoms MSA - Broadband and Home Phone	**Chasing** On Hold - Pending Fujitsu Retail completion
CACI Ltd	Data Micro Segmentation POC	**Investigation** POL considering relationship with CACI and then will remediate as required
UKVI – Overseas	Biometric Enrolment - Overseas Applicants - FOCS Framework	**Investigation** FOCS framework now agreed POL to action with supplier
UKVI - Domestic	Biometric Enrolment - Overseas Applicants - FOCS Framework	**Investigation** FOCS framework now agreed POL to action with supplier
SIA (Security Industry Authority)		**Investigation** FOCS framework now agreed POL to action with supplier

12

POL00423684

www.pwc.com

Post Office Limited
Audit Strategy Memorandum

Year ending 29 March 2020

Audit and Risk Committee Meeting

25 November 2019

pwc

POL00423684

pwc

The Audit and Risk Committee
Post Office Limited
Finsbury Dials
20 Finsbury Street
London
EC2Y 9AQ

Dear Members of the Audit and Risk Committee,

I am pleased to present our Audit Strategy Memorandum (the "Plan") for Post Office Limited and its subsidiaries ("Post Office" or "the Group") for the year ending 29 March 2020 ("2019/2020").

The purpose of this report is to formalise and confirm our proposed audit approach and to give the Audit and Risk Committee the opportunity to understand and comment on the proposed plan. Specifically, the Plan summarises:

- Our approach, including changes to IT scope and risks from prior year, and an updated assessment of the significant and elevated risks relevant to the audit and our proposed responses;
- An overview of the timetable; and
- Other required communications, including independence and responsibilities in relation to fraud.

Our Plan is largely consistent with the previous year, updated to reflect learnings from our first year as your auditor, and will continue to evolve to reflect any changes in the Group or the external market between now and the period end and we will update you of any key changes at future meetings.

I look forward to discussing our Plan with you at the Audit and Risk Committee meeting on 25 November 2019.

GRO

Andrew Paynter
Partner

M: Carla Stent
E: GRO

Yours sincerely

GRO

Andrew Paynter

PricewaterhouseCoopers LLP is a limited liability partnership registered in England with registered number OC303525. The registered office of PricewaterhouseCoopers LLP is 1 Embankment Place, London WC2N 6RH. PricewaterhouseCoopers LLP is authorised and regulated by the Financial Conduct Authority for designated investment business.

POL00423684



Contents

Executive summary	1
Our audit approach	2
Timetable and reporting	16
The Post Office audit team	17
Appendices	18

POL00423684

1. Executive summary

Our evolving audit for the Post Office

The following pages set out our approach for the audit of the Post Office for 2019/2020. This approach is largely consistent with that of the prior year. Notwithstanding this, we continue to evolve our approach to reflect changes in your business and the latest market and regulatory developments but also to ensure our audit remains robust, relevant and insightful.

Whilst auditing standards and what we are required to do remain largely unchanged, how we do it continues to evolve.

We outline some of those changes and how we see they can benefit your audit in section 2.

We will work with management throughout the audit to ensure that our planning is updated to reflect any significant changes in the Group.

Acceptance

Our audit starts with a re-evaluation and assessment of your business and an assessment of overall audit risk. This also pinpoints areas of potentially heightened risk. Our overall conclusion is that audit risk is broadly consistent with that of the prior year, albeit with heightened risk relating to the Postmasters litigation and the requirement to renew the BEIS facilities in the months after the year-end. See section 2 for further details of our risk assessment.

Team

Our team includes good continuity of key team members (including Andrew, Stewart, Rosie and Dan) and a balance of relevant industry experience. It is also supplemented by specialists in areas such as pensions, valuations and other relevant areas as we see appropriate.

Our core team now includes Sarah Allen, as group senior manager role, with Lucy Mason now on maternity leave. An overview of the team structure is given in section 4.

Risk assessment

We have determined the audit risks for the Post Office and included our preliminary assessment of the significant and elevated audit risks, as summarised in section 2.3, together with our proposed approach to address these risks.

Consistent with prior years, we have identified significant audit risks in relation to impairment of fixed assets and impairment of intangible assets subject to amortisation. In line with auditing standards, the risk of management override of controls and the risk of fraud in revenue recognition (across all revenue streams) are also prescribed as significant risks, and we do not rebut these on the Post Office audit. We have identified two additional significant risks relating to Postmasters' Group Litigation Order ('GLO') and Going Concern, which are discussed in further detail on page 4.

Elevated audit risks are also set out within section 2.3. We welcome the Audit and Risk Committee's views on our risk assessment.

Materiality

Our overall materiality for the Post Office has provisionally been set at £9.9 million (2018/2019: £9.7 million), based on a benchmark of 1% of forecast revenue for the 2019/2020 year. We plan to use performance materiality of £7.4 million (2018/2019: £6 million) to direct our testing, which includes a lower "haircut" on overall materiality than in the prior year (25% instead of 37.5%). This reflects the fact that is now our second year as auditors. We will report to you any uncorrected misstatements in excess of £490,000 (2018/2019: £484,000).

Testing approach

Our testing approach is tailored to the systems, transaction and control environment of the Post Office. We consider each financial statement line item separately and design a specific approach appropriate to the assessed risk. Our approach utilises a mix of IT and manual controls work, analytical procedures and substantive testing. We will incorporate data auditing techniques over key audit areas such as journals to provide high quality and effective audit evidence.

Based on our initial discussions, we are planning to rely on IT General Controls for Horizon Online System, Credence and the Agency Billing Module, which sits within CFS. We also plan to rely on the interfaces between Horizon and CFS, and Horizon and Credence, which have been identified as critical for the revenue business cycle.

Based on the above and the detailed walkthroughs conducted as part of our planning procedures, our audit approach will consist predominantly of substantive procedures, which includes detailed testing of all the reports obtained for audit evidence from the other systems, and reliance on management controls and IT dependencies related to Horizon and Credence systems, leveraging from controls where it is efficient to do so.

Fees and non audit fees

Our fee proposal for the 2019/2020 year end audit is currently under discussion with management and we will update the audit committee accordingly. We have included a summary of non audit services provided so far this year in appendix 1.

POL00423684

2. Our audit approach

2.1 Client acceptance and independence

Acceptance risk

Our audit planning process starts with our client acceptance procedures which include an evaluation of the overall risk profile of the Post Office. This includes a high level risk assessment and considers a series of questions covering financial condition, industry risk, competitive position, as well as areas such as management effectiveness, integrity and governance.

As reported to the Audit and Risk Committee in the prior year, we consider there is a higher risk associated with the audit of the Post Office given the high profile and diverse nature of the Group's operations. Our overall conclusion is that audit risk is heightened, which is consistent with that of the prior year, reflecting the fact that the Group continues to work towards becoming a self-sustaining company, free of public subsidy and also reflects the two additional significant risks considered relevant this year. Our risk assessment is summarised in appendix 4.

Independence

Auditing standards require that Andrew Paynter, as our audit partner, considers whether adequate arrangements are in place to safeguard objectivity and the firm's independence. We confirm that, in our opinion, we are independent of the Group, and that there are no matters which would impact our independence and objectivity.

We also confirm that appropriate safeguards are in place in respect of all non-audit work and that in our professional judgement, as at the date of this report, we are independent with respect to the Group within the meaning of UK regulatory and professional requirements and that our objectivity is not impaired in any way. See appendix 1 for further discussion of the non audit services provided to the Group.

Engagement terms

We are engaged to audit the Post Office Limited company and its consolidated financial statements prepared under IFRS. We also audit the Group's subsidiaries' financial statements which are prepared under FRS 101.

2.2 Business understanding

Understanding the Group

We seek to develop a strong understanding of your business, including having a detailed working knowledge of your structure and operations. In developing our audit plan we have spent significant time with the finance team and other key stakeholders and management in the business, and have a number of other meetings planned. This, alongside our detailed walkthroughs of key business processes, has enabled us to strengthen our understanding of your business and control environment, confirm our views on relevant audit risks and develop appropriate responses to those audit risks.

We have retained a high degree of continuity throughout our team to retain business understanding obtained in our first year audit in 2018/2019. See section 4 for the wider team structure.

The Group offers a diverse range of products and services across retail, financial services & telecoms and insurance, and is therefore exposed to a variety of sector specific factors and market dynamics. Whilst trading performance has improved in recent years, with the new banking framework agreement in 2019 providing further forward momentum, the Group also faces headwinds in certain of its business. In addition the long-running Postmasters' Group Litigation Order is reaching a critical stage and the Group will also be renewing its financing facilities with BEIS, which are due to expire on 31 March 2021. We also note that McKinseys are currently assisting the new CEO with a strategic review of the Group, which may give rise to changes in focus and structure in the future.

The pace of regulatory change continues. Conduct risk is an area of constant focus, with many regulated organisations (such as Post Office Insurance ("POI")) seeking to recognise and understand the impact of industry developments. In addition, outsourcing and the use of appointed representatives is also an area of regulatory focus. High profile operational risk failures, including issues in respect of IT resilience and cyber continue to impact the reputation of financial services firms. Complexity of systems, the presence of old legacy systems and manual workarounds increase the risk of control breakdown. Gary Shaw who continues as our POI engagement leader, will present a separate Audit Plan to the Audit & Risk Committee of Post Office Insurance.

POL00423684

2.3 Relevant risks

Our risk assessment process seeks to identify key risk areas and to determine how much audit evidence is required in each area. During the process we consider:

- Macro-level factors and their capacity to impact operations, financial reporting and compliance; and
- Business specific risk drivers and their potential impact on financial reporting.

As required by Auditing Standards, we have carried out a risk assessment for 2019/2020 prior to considering the mitigating impact of controls that you have in place. Our risk assessment draws on our cumulative knowledge of the group (including key changes in the business from the prior year), our prior year audit experience, our understanding of key judgements in your industry and the results of your own risk assessment exercise.

We determine if audit risks are significant, elevated or normal and whether we are concerned with fraud, error or judgement. This subsequently drives the design of our testing procedures. Significant audit risks are those with the highest potential for material misstatement due to a combination of their size, nature and likelihood and which, in our judgement, require specific audit consideration.

Potential risk of fraud

In accordance with Auditing Standards, we plan and perform our audit so that we have a reasonable expectation of detecting material misstatements in the financial statements or accounting records, including any material misstatements resulting from fraud, error or non-compliance with law or regulations.

Three conditions are generally present when fraud occurs:

- Management or other employees have an incentive, or are under pressure, providing a reason to commit fraud;
- Circumstances exist (e.g. the absence of controls, ineffective controls, or the ability of management to override controls) that provide an opportunity for a fraud to be perpetrated; and
- Those involved are able to rationalise a fraudulent act.

The respective responsibilities of auditors, management and those charged with governance are outlined in appendix 3.

Our understanding of specific fraud risks in relation to the Post Office:

The group's business is characterised by a high volume of low value transactions at a consumer level (i.e in branch). This gives rise to a lower risk of material fraud at the transactional level. However, when considering certain revenue streams that have a large fixed price element, e.g. with the contract with Royal Mail, there is a risk of fraud at the centralised financial reporting transactional level. See pages 4 and 5 for further details.

Management are also incentivised on the Group's performance and there is potential pressure to meet stakeholder expectations. We therefore also consider specific fraud risks that could be material to the Group's financial statements in the following areas:

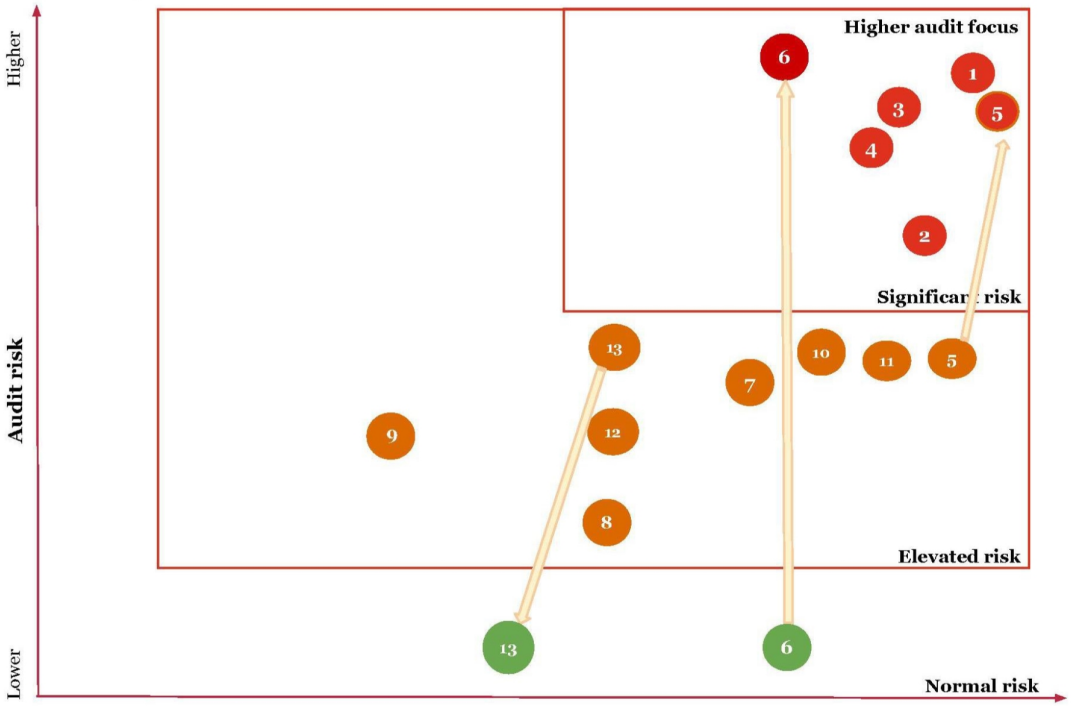
- Manipulation of financial results through posting of inappropriate journals;
- Key assumptions used which have a significant impact (for example, in the impairment model); and
- Significant judgements applied in other areas of estimation.

POL00423684

2.3 Relevant risks (continued)

For those risks that we have assessed as an audit risk, we have considered whether they give rise to an elevated or significant risk as described below. This assessment is performed for each individual financial statement line item. Further detail of our assessment of risk, and our proposed approach, is detailed in the following pages. We have also presented our full risk strategy summary by individual financial statement line item in appendix 4.

Group risk assessment



	Identified risk
1	Risk of management override of control*
2	Fraud in revenue recognition*
3	Impairment of intangible assets subject to amortisation
4	Impairment of fixed assets
5	Postmaster litigation
6	Going concern
7	Impairment of goodwill - POMS
8	Capitalisation of intangible assets
9	VAT accounting
10	Assumptions in the pension schemes' liabilities
11	Classification and recognition of Trading Profit
12	IFRS 16 - first year full adoption
13	Fair value of assets relating to Payzone acquisition

* These risks are required by auditing standards, applicable to all audits.

- *Going concern has increased to a significant risk in 2019/2020, reflecting the expiry of the current facilities in March 2021.*
- *Postmaster litigation has increased to a significant risk during the year reflecting the progress of the trials / possibility of settlement and the likelihood that management may need to book a provision.*
- *In the prior year we identified an elevated risk relating to Payzone acquisition accounting which has reduced to a normal risk this year. Accounting standards allow twelve months to 'true up' any fair value accounting, but due to the size of balances involved this is likely to be immaterial.*

Significant risk	***Elevated risk***
These require specific focus in the year, usually because they require significant judgements or are not routine. Testing includes an evaluation of the controls in place as well as substantive testing.	Although not considered significant, the nature of the balance/area requires specific consideration.

In addition to the above identified significant and elevated risks, we will spend time auditing all material balances and there will be a specific focus on Network cash, key account reconciliations, recoverability of accounts receivable and accruals. We will also review large significant contracts and how these are being managed by the Group.

POL00423684

2.3 Relevant risks (continued)

Audit risks	Our assessment and planned response	Audit risk assessment 2019/2020	Audit risk assessment 2018/2019
Management override of controls (All assertions - pervasive risk)	This risk is required by auditing standards – it is therefore classified as a significant risk on every audit engagement. This risk is pervasive over the financial statements and could potentially affect all financial statement line items. • We will test a sample of journal entries using our data analytics tool 'Halo for Journals' that have been identified as a potentially higher risk, for example, items that credit the P&L with a corresponding debit to an 'unusual' balance sheet account. • We will investigate and understand the reason for any significant, unusual or one-off transactions. • We will review segregation of duties across relevant financial reporting processes. • We will perform detailed testing over year end reconciliations. • We will review the accounting for any significant estimates and areas of judgement to assess and challenge their appropriateness. This will include consideration of any centrally held provisions, including those that are immaterial. • Performing procedures outside of the typical testing plan will also be incorporated to ensure an element of unpredictability.	• Significant	• Significant
Fraud in revenue recognition	Similar to the above, auditing standards also presume that we regard this as a significant risk on all audits where the risk cannot be rebutted. Given the volume of revenue transactions across a variety of different streams (including retail, financial services & telecoms, and insurance) this will be an area of focus. We have included a detailed assessment by type of revenue in Appendix 4 which is summarised as follows: 1. ***Fixed contractual (existence/ occurrence)*** - This relates to contracts with customers such as Royal Mail, which includes a fixed contractual amount (as well as variable commission amounts which form part of 'Horizon to Credence' below). The risk of fraud is considered to exist at a journal level rather than at a transactional level and will therefore be responded to through the testing of unexpected journals to revenue. 2. ***Horizon to Credence (existence/ occurrence, cut off)*** - This revenue stream relates to commission earned on goods and services sold by the Post Office on behalf of other entities (for example lottery tickets sold on behalf of Camelot). Revenue consists of a large volume of smaller transactions on Horizon, that are combined on larger value invoices therefore the risk of fraud is considered to exist at a journal level as well as at the invoice (but not individual Horizon transaction) level and tested as above. We will also perform testing over the reconciliations and commission rates, leveraging from the ITGC testing performed over the systems where appropriate and efficient. 3. ***Direct to CFS (existence/ occurrence, cut off)*** - Revenue recognised directly in CFS includes revenue such as Identity and Payment Services, whereby the transactional data from Horizon interfaces directly into CFS through the Agent Billing module. The risk of fraud is at the journal level rather than transactional level and tested in a consistent way to the Horizon to Credence revenue stream above. 4. ***Reliance on third parties (existence/ occurrence, cut off)*** - Post Office recognise some of their commission revenue based on the amounts communicated to them by the third parties whose products they are selling such as Bank of Ireland, Moneygram and FRES. The third party takes the sales data from the Post Office and calculates the commission owed. Consistent with the above, the risk of fraud is at a journal level. 5. ***Telecoms (existence/ occurrence)*** - Post Office's telecoms revenue relates to Post Office branded broadband and home phone services provided to customers through the network access providers, TalkTalk and BT. Fujitsu are a third party who provide administrative services, including the billing which has some complexity due to the different plans available to customers. The risk of fraud is again at a journal level.	• Significant	• Significant

POL00423684

2.3 Relevant risks (continued)

Audit risks	Our assessment and planned response	Audit risk assessment 2019/2020	Audit risk assessment 2018/2019
Impairment of intangible assets subject to amortisation (Valuation)	The Post Office holds a significant amount of intangible assets on the balance sheet which primarily relate to software costs of £228 million at the 2018/2019 year end (2017/2018: £213 million). There was significant spend in 2018/2019 for costs incurred to bring new systems into place as part of the BOT project. Intangible asset additions in 2019/2020 remain substantial at £32 million as at October 2019. Impairment reviews are required to demonstrate that the ongoing value for different elements of the project can be supported, and that new elements are not superseding previously capitalised assets. • We will understand and test management's impairment assessment and consider whether any other impairment indicators exist such as changes in design or changes in anticipated benefits. • We will review progress to date and understand if any costs incurred over the budget suggest a potential impairment provision is required.	• Significant	• Significant
Impairment of fixed assets (Valuation)	The Group holds a significant balance in relation to property, plant and equipment of £176 million at the 2018/2019 year end. In addition, the asset base is due to increase in 2019/2020 as a result of IFRS 16, with the Post Office expecting to recognise a right of use asset in relation to their lease portfolio of over £75 million. Accounting standards require management to assess the possibility of an impairment charge trigger or any reason why it may be appropriate to reverse previously booked impairment charges. This would take into account current trading performance, and also consider other factors such as external economic conditions, specific conditions related to individual trading branches and market interest rates. The challenging trading environment, coupled with the Group's historic trading performance, could present an impairment trigger for the Post Office's branch asset portfolio. • We will assess management's allocation of cash generating units ('CGUs') for reasonableness and appropriateness, including the assumption that there are only two CGUs, Post Office Limited and Post Office Management Services Limited, rather than a third for Payzone. • Our work will focus on the audit of the cash flow models and the underlying judgements and assumptions applied. We will challenge the key assumptions underlying the impairment model, in particular, the composition of cash flows, growth rates and the discount rate.	• Significant	• Significant
Postmaster litigation (Rights and Obligations/ Valuation)	The Post Office has an ongoing litigation order with a number of postmasters which resulted in contingent liability disclosures in the 2018/2019 accounts. Two trials have taken place with the first judgement in favour of Postmasters and the second due in November. The GLO is a highly uncertain situation which could, based on past events, lead to a material economic outflow from the Group. At the time of writing this report, there remains a lack of clarity as to the ultimate outcome, however it is possible that circumstances change quickly in the coming months and give rise to the need for a provision to be booked in the 2019/20 financial statements. • We will discuss and understand the status of the claim with management including their rationale as to whether a provision should be recognised. • The outcome of all trials will be reviewed as they become available. • If a provision has been recognised we will discuss and validate the assumptions used to calculate it with management to ensure the principles and treatments used are appropriate. • We will obtain legal correspondence and hold discussions with the Group's legal advisors to corroborate management's assumptions and any related disclosures.	• Significant	• Elevated

POL00423684

2.3 Relevant risks (continued)

Audit risks	Our assessment and planned response	Audit risk assessment 2019/2020	Audit risk assessment 2018/2019
Going concern	The Group has a £950 million working capital facility with BEIS which is due to expire on 31 March 2021. This date is within 12 months of the planned date for signing the financial statements (in the summer of 2020). In addition, the final Network Subsidy Payment per the current agreement, of £50 million will be received from BEIS in the 2020/2021 financial year, and any amounts receivable going forward have yet to be agreed. As the Post Office is currently reliant on BEIS funding as its principal source of finance (and therefore to continue as a going concern), we have determined that the Going Concern assumption should be considered a significant risk. We will continue to assess the risk profile, with a view to de-risking this to a normal level if BEIS financing is formally in place prior to signing the Group's 2019/2020 accounts. • We will review management's detailed going concern paper, assessing the reasonableness of cash flow forecasts, security headroom and the other assumptions used. • We will perform sensitivity analysis over the assumptions applied in the forecast. • We will review forecast covenant compliance for any potential breaches. • We will consider opportunities available to management to mitigate any going concern risk.	Significant	Normal
Accuracy of telecoms revenue (Accuracy)	In addition to the fraud risk relating to revenue, due to the complexity of billing, we have identified a significant risk in relation to accuracy of telecoms revenue. • We will test a sample invoices to high assurance and corroborate to signed contracts and pricing plans.	Significant	Significant
Impairment of goodwill - POMS (Valuation)	At a Post Office Management Services Limited (POMS) level there is a goodwill balance of £43.9 million (2018/2019: £43.9 million) that relates to the acquisition from the Post Office Limited of its former insurance contractual arrangement with the Bank of Ireland. This risk is relevant at both the Company and Group levels as it is recognised in both sets of financial statements. • We will review management's justification for the carrying value, assessing the reasonableness of cash flow forecasts and other assumptions used. • We will challenge the key assumptions underlying the impairment model, seeking to reach agreement on key judgements such as discount rate and others in advance of the year-end, and will perform sensitivity analysis.	Elevated	Elevated

POL00423684

2.3 Relevant risks (continued)

Audit risks	Our assessment and planned response	Audit risk assessment 2019/2020	Audit risk assessment 2018/2019
Capitalisation of intangible assets (Accuracy/ Existence)	As a result of BOT in the prior year, there was a significant increase in software costs during the 2018/2019 year end. Whilst BOT is now complete, other projects have continued into the 2019/2020 year end, with additions of £32 million as at October 2019. Accounting standards dictate specific criteria that costs need to meet to be capitalised as an intangible asset and this creates a risk of misstatement. • We will perform detailed testing of the additions in the year to ensure they meet the recognition criteria and have been capitalised appropriately, paying particular attention to the capitalisation of labour costs.	• Elevated	• Elevated
VAT accounting (Accuracy)	Due to the different divisions and revenue streams within the Post Office, there are a number of arrangements in relation to VAT. However as there is minimal judgement involved we have deemed this an elevated risk rather than significant. • We will obtain the VAT arrangements in place and review the latest correspondence with HMRC. • We will test a sample of transactions to ensure the appropriate rate has been applied. • Where required, we will engage with VAT specialists to review complex arrangements and assist in testing the compliance.	• Elevated	• Elevated
Assumptions in the pension schemes' liabilities (Valuation/ Presentation and disclosure)	The Post Office Limited holds two defined benefit schemes both of which are in a net asset position. The main scheme assets are capped which resulted in a £1 million (2017/18: £3 million) asset being recognised on the balance sheet in 2018/2019. There will be a number of judgements and estimates made by management (in conjunction with the actuaries) when valuing the scheme as at 29 March 2020. The key drivers of the liability of both schemes are the discount rates, inflation and mortality assumptions. In addition, there is a significant estimate applied to the RMSEPP scheme, whereby Post Office recognise 7% of the multi-employer scheme's assets and liabilities. • We will audit the key judgements and membership data used to value the schemes' liabilities. • We will review the financial statement disclosures for completeness and accuracy and to ensure they align with accounting standards. • We will review management's assessment of the right to recognise the net surplus under the requirements of IFRIC 14. • We will consult with our independent pensions specialists as required.	• Elevated	• Elevated

POL00423684

2.3 Relevant risks (continued)

Audit risks	Our assessment and planned response	Audit risk assessment 2019/2020	Audit risk assessment 2018/2019
Classification and recognition of Trading profit (Accuracy/ Presentation and disclosure)	The Group uses "Trading Profit" as its key alternative profit measure and it is calculated by taking operating profit from continuing operations before depreciation, amortisation, operating exceptional items, closure of activities, investments and Network Subsidy Payment. Furthermore the Group uses a three column approach in its income statement in order to segregate what it considers underlying results. The use of the columnar approach is to inform the users of the accounts on how the investment funding from BEIS has been spent. There is judgement in the classification of relevant costs and income which therefore carries audit risk. The Post Office will receive the final instalment of investment funding of £42 million in 2019/2020 (2018/2019: £168 million). For subsequent periods management expects the columnar approach will cease. • We will obtain an understanding of management's criteria and accounting policy in relation to recognising costs within the 'Investments' column of the Income Statement. • We will corroborate a sample of these costs to supporting documentation to ensure they meet the criteria and are not inappropriately classified within 'Investments'. • We will obtain an understanding of management's approval process and perform walkthroughs in relation to investment expenditure. • We will obtain an understanding of management's criteria and accounting policy in relation to recognising costs within the 'Investments' column of the Income Statement. • We will understand and review the nature of the majority of the different projects, through discussions with project managers, finance and review of board reports, to ascertain whether they meet the definition of the relevant programme at a high level. • We will trace all material projects included within the investments column to the quarterly funding reports presented to the Board. • We will corroborate a sample of costs (across a number of different projects, including smaller ones) to supporting documentation to ensure the existence of these costs, that they meet the criteria and that they are not inappropriately classified within 'Investments'. • We will utilise our "Halo for journals" data analytics software to identify any journals that have debited investments and credited operating expenses (i.e. increasing spend in the investments column and decreasing "normal" operating expenses). • We will corroborate a sample of payroll costs included within 'Investments' to ensure these employees have been working on the projects that sit within the programmes.	Elevated	Elevated
IFRS 16 - first full year adoption (Valuation/ Presentation and disclosure)	The Group will be applying IFRS 16 for the first time at the 2019/2020 year end using the simplified transition approach to implementing IFRS 16. In 2018/2019 management disclosed the expected impact on adoption in line with IAS 8. The lease liability and pre impairment right of use asset was estimated to range between £75 million and £85 million. Due to the magnitude of the expected balances and the judgmental assumptions applied in relation to the implementation of IFRS 16, this has been deemed an elevated risk. • Our work will focus on the audit of the complex model and underlying judgements taken. • We will evaluate the model's key assumptions, most noticeably the discount rate of 3%, taking into account the specific characteristics of the Group's leases, and utilise our valuations experts, where appropriate. • We will perform sensitivity analysis over key judgements to assess the impact of reasonable possible changes in assumptions that would impact the range disclosed. • An exercise will be performed to gain comfort that a complete listing of leases within the Group has been incorporated into the model. • The disclosures will be reviewed to determine that these are in accordance with accounting standards, including the reconciliation between the 2018/2019 operating lease commitment note to the IFRS 16 note.	Elevated	Elevated

POL00423684

2.4 Intelligent scoping

Audit quality, effectiveness and business insight are the result of an intelligently scoped audit with the right focus on the higher risk areas. We have a well-developed approach which is designed to ensure we obtain the 'appropriate' level of audit evidence for each financial statement line item.

Building on all the essential pieces of information gathered such as materiality, risk, size, complexity and structure, we determine our scope. This covers what we do, the best types of audit evidence to obtain, the right areas of your operations to focus on and the best people needed to deliver this.

Scoping

Scoping covers where we go and what we do, the best types of audit evidence to obtain, the right areas of your operations to focus on and the best audit resources needed to deliver this. We use our Smart Planning approach and software to create the optimal scope and to ensure our audit is as effective and efficient as possible.

We will perform a full scope statutory audit of all the Group companies below. We have detailed in the table below the entities that are financially significant components as defined by auditing standards and that require a full scope audit.

Legal entity	Full scope audit required for Group audit opinion?
Post Office Limited	✓
Post Office Management Services Limited	✗
First Rate Exchange Services Limited	✓
Payzone Bill Payments Limited	✗

For the purpose of the group audit opinion we will not be performing any audit procedures over Payzone due to the minimal financial impact on the consolidated accounts.

Post Office Management Services Limited is not considered a significant component of the Group, however we have concluded that the goodwill balance is material to the Group, therefore audit procedures over the goodwill balance will be performed for the Group audit by the component team, led by Gary Shaw (POI engagement leader) .

First Rate Exchange Services Limited is a joint venture and will again be audited by KPMG. This will include both their statutory audit opinion and the procedures required for the group audit opinion. We will instruct them to perform a full scope audit for the period ending 29 March 2020. See appendix 7 for our expected reporting timetable.

Materiality

In line with the requirements of ISA 320 'Materiality in Planning and Performing an Audit' our audit procedures are planned to address the risk of, and identify, material misstatement within the consolidated financial statements. Our preliminary overall materiality level has been set at £9.9 million (2018/2019: £9.7 million) based on 1% of the Group's budgeted revenue for the 2019/2020 year. We have considered other benchmarks on which to base our materiality, for example weighted average profits and APMs, but due to the volatility of these measures, and the relative stability of revenue, revenue is considered to be an appropriate benchmark. The final materiality figures will be based on the actual results and any significant changes will be communicated to the Audit and Risk Committee.

In planning our audit procedures, we take into account the risk of the aggregation of errors, being a number of smaller errors which may, in aggregate, result in a material misstatement within the consolidated financial statements. As a consequence, performance materiality is set below overall materiality.

Performance materiality is used in the scoping of our work and determining our sampling selection. This is calculated as 75% (2018/2019: 62.5%) of overall materiality, being £7.4 million (2018/2019: £6.0 million). As part of our planning procedures we determine the haircut applied to overall materiality by considering a number of factors including, history of misstatements, risk assessment and aggregation risk and effectiveness of controls. In the prior year, we calculated overall materiality using the same revenue benchmark, however applied a 37.5% haircut in calculating performance materiality due to it being a first year audit. We have determined based on prior year experience that a 25% haircut is appropriate this year, as there were minimal adjustments identified in the 2018/2019 year end audit.

	2019/20 £m	2018/19 £m
Overall materiality	9.9	9.7
Performance materiality	7.4	6.0
Adjustment posting threshold	0.5	0.5

Communication of potential differences

Where potential adjustments are identified, their impact on the financial statements will be assessed (for example incorrect disclosures or a misstatement to a particular financial statement line item). All identified misstatements above the de minimis level will initially be communicated to management for discussion and resolution. In line with the requirements of ISA 260 'Communication with Those Charged with Governance' we will discuss all identified misstatements unless they are below the de minimis level. With the agreement of the Audit and Risk Committee, we would anticipate reporting on all individually identified misstatements above £490,000 (2018/2019: £484,000) - being 5% of overall materiality. We will also report on any omitted, incomplete or inaccurate disclosures in the financial statements and/or other information that are above a clearly trivial level.

POL00423684

2.5 Robust testing

The Post Office audit

Our approach optimises the balance between tests of detail, controls testing, analytics and data techniques. The mix of each of these is largely dependent on the quality and structure of your financial control environment, along with the assessed level of risk. As a result, we have a bespoke testing plan for all balances within your financial statements.

What we plan to do

Testing IT and systems

Our work over IT General Controls ("ITGCs") considers the underlying systems environment (applications, databases and operating systems) of key financial reporting applications.We tailor our approach to our ITGC audit based on the extent to which reliance can be placed on automated procedures and controls within system calculations, system generated reports, automated controls, security (including segregation of duties) and interfaces between systems.Where these procedures can be relied upon, the level of our substantive testing can be reduced and efficiencies in our audit approach can be achieved.

Consistent with 2018/2019, to support our revenue testing approach we are seeking to place audit reliance over the Horizon and Credence systems and their inherent controls for 2019/2020. By testing these controls we increase our level of comfort over the systems output used in the audit, leading to a reduction in the substantive testing required.

We have also planned to test interfaces between Horizon and the systems, Credence and CFS, which were identified during our process understanding as critical interfaces for the Revenue cycle. We are also revising our approach to agency remuneration, and assessing the possibility of obtaining ITGC comfort over the new Agency Billing module within CFS following the completion of the BOT programme in 2018/2019.

Testing of controls

As well as looking to test and rely on system controls, we will also continue to seek to test and place reliance on a number of manual controls you have operating in the business, particularly in the cash and payroll areas.

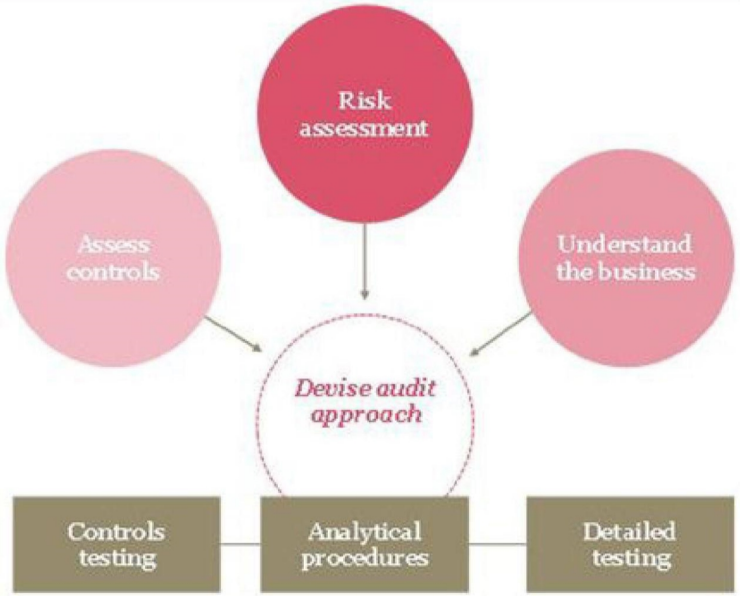
Substantive testing

We will always supplement any controls comfort with further tests of detail, ensuring our overall testing continues to provide robust assurance over the financial statements. Where we have assessed audit risks as elevated or significant we will perform higher levels of substantive work.

Within appendix 4, we have detailed our audit approach per 'FSLI' (financial statement line item) showing the relative balance of controls and substantive testing.

Related parties

Auditing standards require us to plan and conduct our audit so that we obtain sufficient appropriate evidence about whether related party relationships and transactions have been appropriately identified, recognised and disclosed in the financial statements. To do this effectively, we have obtained a related party list from management as part of our planning procedures, which will be updated in April prior to the commencement of the audit.



Use of experts and specialists

Where your transactions or account balances are complex or subject to complicated accounting rules, we ensure we have the right balance of skills to audit these areas.

We have access to a broad range of industry, accounting and subject matter experts and we use experts and specialists within PwC to assist in our audit work in specific areas where more specialist knowledge is needed, including:

- IT specialists to undertake an audit of the core IT systems where applicable;
- Data specialists working as part of the audit team to deliver effective data auditing testing;
- Pensions valuations specialists who assist in assessing reasonableness of actuarial assumptions;
- Pensions specialists to audit the plan assets of the pension schemes;
- Valuations specialists may be used to assess the reasonableness of the discount rates used in, IFRS 16 and impairment models. They will also validate the fair value of any derivatives held at year end; and
- Other specialists, such as VAT specialists as and when required.

POL00423684

2.5 Robust testing (continued)

The following table shows our approach to the 2019/2020 systems audit, specifically where we will seek to place reliance in 2019/2020 and how this differs from our prior year approach.

Where the systems below are flagged as 'In Scope,' we will take an IT General Controls ('ITGCs') approach, which means we will consider the underlying systems environment (applications, databases and operating systems) of key financial reporting applications. We will then tailor our approach to our ITGC audit based on the extent to which reliance can be placed on automated procedures and controls within system calculations, system generated reports, automated controls, security (including segregation of duties) and interfaces between systems. Where these procedures can be relied upon, the level of our substantive testing can be reduced and efficiencies in our audit approach can be achieved.

System Name	System Functionality	Key Connecting Systems	2018/2019 Approach	Proposed 2019/2020 Approach	2019/2020 Audit work required (if different to 2018/2019)
SAP CFS (ECC6.0)	General Ledger; Accounts Payable; Accounts Receivable; Asset Accounting; Purchase to Pay; Treasury; Agent Remuneration (SAP ICM); Settlement and Billing and Profitability Reporting.	Credence / Horizon / CWC	Out of Scope: BOT Programme	Out of Scope	As part of planning, we have reviewed the reports generated from CFS that were used as part of the 2018/2019 audit to assess whether we can gain any efficiencies by obtaining ITGC comfort over CFS. As the large majority of transactional data (revenue, client receivables and payables, cash) is driven from Horizon and Credence, there are minimal reports from CFS used as part of the audit. We expect the reports we require from CFS will be limited to Accounts payable and Accounts receivable. Each report taken from CFS and used for audit evidence will need to be tested for accuracy and completeness.
POL SAP (4.7)	Client settlement and Billing processes and Partner Payments (functionality to be migrated to CFS)	N/A	Out of Scope: BOT Programme	N/A (System Retired)	N/A as client settlement and billing processes and Partner Payments moved to CFS.
SAP HR (4.7)	Agent Remuneration (functionality to be migrated to CFS)	N/A	Out of Scope: BOT Programme	N/A (System Retired)	N/A as agent remuneration moved to CFS.
Transtrack CashWeb Community (CWC)	Cash Management	CFS	Out of Scope: BOT Programme	Out of Scope	N/A as a result of the ongoing issues. Whilst the differences arising from the CWC issues have reduced, it is unlikely we will be able to rely on ITGCs for this system.
Horizon (HNGX/HNGA)	Revenue	Credence / CFS	In Scope	In Scope	Main branch revenue system - no additional audit procedures are expected to be performed.
SAP Success Factors	Employee Payroll; Employee Master Data; Talent and Recruitment	CFS	Out of Scope: Inefficient Audit Approach	Out of Scope: Inefficient Audit Approach	Consistent with the prior year, SAP Success Factors is out of scope and instead we deem a substantive approach to be most efficient. We will reconcile payroll reports to the general ledger and perform substantive testing procedures over payroll costs. In addition we will perform testing over starters and leavers.

POL00423684

2.5 Robust testing (continued)

System Name	System Functionality	Key Connecting Systems	2018/2019 Approach	Proposed 2019/2020 Approach	2019/2020 Audit Work Required (if different to 2018/2019)
Credence	Financial Reporting System	Horizon / CFS	Out of Scope: BOT Programme	In Scope	We do not expect additional audit procedures to be performed, but if concluded that that ITGC reliance cannot be obtained, then further substantive analysis would need to be performed to ensure that key financial IT dependencies are complete and correct.
Agency Billing module	Module which contains the details of Agents Revenue and Remuneration	Horizon / CFS	Out of Scope: BOT Programme	In Scope	We do not expect additional audit procedures to be performed, but if concluded that that ITGC reliance cannot be obtained, then further substantive testing would need to be performed to ensure that key financial IT dependencies are complete and correct.

POL00423684

2.5 Robust testing (continued)

Data auditing

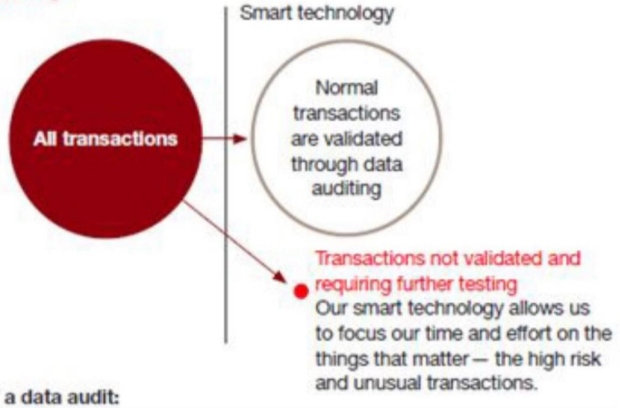
We will continue to use data audit techniques to enhance the precision of our audit procedures as well as the overall coverage we obtain from our testing. These techniques enable us to interrogate all transactions in a population and identify 'higher risk' transactions – for example those not calculated properly, transactions that do not follow the expected information flows or do not offset to appropriate balance sheet accounts. We are able to target our detailed testing towards these higher risk transactions as opposed to simply performing a sample across all transactions. We are planning on using data techniques in the audit of journals. See further details below.

Halo for Journals

As part of journals testing, we will use our technology based tool, "Halo for Journals," which helps to identify higher risk transactions and process inefficiencies through the use of algorithms. This technology can interrogate journals to reveal relationships and patterns in account codes, individual users, months, times of day, types of journals and amounts.

By being able to interrogate the data, this will help to focus testing on what we perceive to be higher risk areas, thus helping to assess the significant audit risk of management override of controls.

Use of data auditing



The benefits of a data audit:

Quality
- **All** transactions are interrogated and analysed
- Coverage levels from substantive tests increased
- Audit effort is **focused** on higher risk transactions

Efficiency
- Testing can be performed off-site and throughout the year

Experience
- Your finance teams spend less time providing us with supporting documentation
- Our audit team gains a better understanding of your business with less time spent on detailed audit testing

Insight
- Visibility is provided over your activities and transactions
- Patterns in your data are identified
- Benchmarking can be performed

POL00423684

2.6 Meaningful conclusions

The essence of providing meaningful conclusions is bringing our knowledge of your operations, the results of our work and our experience of other clients and your industry together to bring relevant and reliable findings. This underpins both successful compliance and our ability to provide useful insight to you.

In designing the Post Office audit, our primary objective is to form an independent audit opinion on the Group financial statements. However, we also aim to provide insight which supports your business evolution.

Audit value comes from the same source as audit quality so the work that we do in support of our audit opinion also means that we should be giving you value through our observations, recommendations and insights.

We propose that we report our final findings to the June Audit Committee, which will include the following:

- Significant audit and accounting matters arising from our work on areas of significant and elevated audit risks, as outlined in section 2.3;
- Key internal control observations and recommendations;
- Results of the IT controls audit;
- Final proposed audit opinion; and
- Any identified misstatements, above our reporting threshold (£490,000).



Good to know

We fundamentally believe in the value of the audit and its crucial role in providing confidence to shareholders. We also believe that value comes from a quality audit. Sharing our views and insight are a key aspect of what we do and how we work with you.

POL00423684

3. Timetable and reporting

August - October

Key activities
- Acceptance and continuance
- Independence assessment
- Planning activities including meetings with management
- Risk assessment
- Scoping of the audit
- Attendance at cash counts

Key communications
- Debrief on the 2018/2019 audit



November - February

Key activities
- Update understanding of the control environment and IT systems
- Test IT systems and controls, where relevant
- Testing of the operating effectiveness of key business process controls
- Update our understanding of all significant balances
- Development of testing plan
- Early audit testing of key areas of focus and interim transactional testing
- Early discussion of key judgements
- Attendance at cash counts

Key communications
- Engagement letters
- Scope of work, timetables and deliverables
- Controls reporting and update on significant audit issues
- Audit Strategy Memorandum presented to Audit and Risk Committee

September - November

Key activities
- Finalisation of the audit testing over the remaining subsidiaries
- Agreed upon procedures testing performed
- Review of the financial statements for the remaining subsidiaries.

Key communications
- Statutory audit opinions for the subsidiaries
- Management representation letters for the subsidiaries
- Agreed upon procedures reports issued

March - June

Key activities
- Year end audit testing onsite
- Attendance at cash counts
- Update on final position of key management models/ assumptions/ estimates
- Review of related party disclosures
- Review of the Group financial statements
- Perform procedures in relation to the Bank of England assurance Engagement
- Receive reporting from component audit teams

Key communications
- Discussion of findings with management
- Year end Audit and Risk Committee Report presented to the Audit and Risk Committee
- Audit opinion and management representation letter

POL00423684

4. The Post Office audit team

Team structure

As in 2018/2019, our team is structured to bring the right combination of specialist skills, experience and innovation to the Post Office audit. It reflects carefully planned succession to ensure that we maintain continuity. Andrew Paynter is Group Audit Partner, supported by Gary Shaw, an experienced Financial Services Partner. As a result of Lucy Mason being on maternity leave during the year, we have brought Sarah Allen onto the team as the Group Audit Senior Manager. All other managers were heavily involved in the 2018/2019 Post Office audit.

Quality Review Partner

To ensure we uphold the highest standards of audit quality, we appoint a Quality Review Partner, who works alongside Andrew in reviewing key documents, our reports to you and any significant judgements.



Experts and specialists

Valuations

Peter Blockley - Manager

Pensions

Louise Dodds - Manager

P&O (Actuaries)

Mike Kippax - Senior Manager

Kevin McDonald - Senior team member

POL00423684

Appendices

Appendix 1 – Non audit fees 19
Appendix 2 – Independence and quality 20
Appendix 3 – Risk of fraud 22
Appendix 4 – Risk strategy summary 23
Appendix 5 – Key communications 26
Appendix 6 – Governance reform and related reporting changes 27
Appendix 7 – Reporting timetable 31

POL00423684

Appendix 1 - Non audit fees

Non-audit fees

We have set out below a summary of non-audit services invoiced to the Group during 2019/2020 year end, and the 2018/2019 comparative (split between pre and post appointment).

Service	£'000 2019/2020	£'000 2018/2019 Pre-appointment February 2019	£'000 2018/2019 Post-appointment
Remuneration committee benchmarking advice	GRO		
Forensics & other accounting support relating to telco			
SAP secondment			
Co-source Internal Audit services			
TrAction			
Other services			
Total			

All non-audit services are subject to PwC's internal independence approval processes, which includes an assessment of any potential threats to auditor independence from the service, together with consideration of the safeguards which mitigate those threats. Each of these require approval from Andrew Paynter before the service can commence and are included on our audit file as a permanent record. We also consider the impact of the services in aggregate on our auditor independence.

For any such non audit services provided, the engagement team have ensured that the required safeguards are in place, for example, separate teams performing the work, and we can confirm we are independent of the Group.

We will provide a full update in the June Audit and Risk Committee detailing each service provided and the level of fees charged.

POL00423684

Appendix 2 - Independence and quality

Quality is built into every aspect of the way that we deliver the audit. We take great pride in being your auditors and in the value of assurance that the audit opinion provides. A timely, independent and rigorous audit is fundamental. This in turn necessitates getting the basics right – clarity on audit risks, scope, resource, timetables, deliverables and areas of judgement – which is supported by our team who have extensive experience and relevant training.

As lead audit partner, Andrew Paynter has overall responsibility for the quality and execution of the Group audit and is accountable directly to the Audit and Risk Committee. In this role, he will:

- Set the tone and expectations of quality to all PwC teams and ensure clear accountability within our team structure;
- Confirm that our teams have complied with the necessary training and with our Group audit instructions; and
- Be notified of any breaches of independence.

We have in place rigorous procedures to safeguard our independence from Post Office and to ensure the quality of our audit. In the UK, these procedures are detailed in our 2019 Governance and transparency report which is published on the PwC website: www.pwc.co.uk/who-we-are/annual-report/governance-and-transparency.html

Procedure	Description
People	Quality begins with our people. To ensure that every engagement team provides quality, we use carefully designed protocols for recruiting, training, promoting, assigning responsibility and managing and overseeing the work of our people. Every team member is carefully selected to ensure they have the right blend of technical expertise and industry experience to support your business and receives a tailored induction to ensure they have a thorough understanding of the significant risks and judgements applicable to the audit. We invest significant amounts of time and money for the training and development of our audit professionals. We are investing an additional £30 million annually as part of a wide ranging action plan to provide greater focus on the quality and public interest responsibilities of PwC's statutory audit services.
Client acceptance and retention	Our client acceptance and retention standards and procedures are designed to identify risks of a client or prospective client to determine whether the risks are manageable.
Audit methodology	The same audit methodology is used for all audit engagements by our member firms, thereby ensuring uniformity and consistency in approach. Compliance with this methodology is reviewed and evaluated regularly. Comprehensive policies and procedures governing our accounting and auditing practice – covering professional and regulatory standards as well as implementation issues – are updated continuously for new professional developments and emerging issues, needs and concerns of the practice. Non-PwC component firms are subject to the same regulatory environment and we, as the group auditor, assess their competence in their role and are sufficiently involved in their audit work to meet our requirements under ISA 600.. We are involved at the planning stage to identify relevant risks and perform a review of the final working papers to ensure that they are in compliance with PwC methodology.
Quality review partner	Your audit has an assigned quality review partner ("QRP"), appointed to have the appropriate experience and expertise, who conducts a pre-issuance review of all significant issues. The QRP undertakes a quality review of our Audit and Risk Committee reports and audit file to assess and challenge our key planning judgements, execution of our response to significant risks and reporting to those charged with governance.
Hot reviewer	The QRP is supported by a hot reviewer, who performs an independent review of the financial statements in addition to the engagement manager, engagement leader and QRP's themself.

POL00423684

Appendix 2 - Independence and quality (continued)

Procedure	Description
Partner rotation	Lead engagement partners are required to rotate off higher risk clients at least every seven years, as required by our own rules and by regulatory bodies. Rotation ensures a fresh perspective without sacrificing PwC's knowledge. Andrew Paynter is in his second year as Group Audit Partner.
Technical consultation	Consultations by engagement teams, typically with senior technical partners unaffiliated with the audit engagement, are required in particular circumstances involving auditing, accounting or reporting matters including matters such as going concern and restatements.
Technical updates	PwC prepares numerous publications to keep both PwC staff and our clients abreast of the latest technical guidance. These include: • A weekly publication covering the week's accounting and business developments. • A periodic publication providing in-depth analysis of significant accounting developments. • A publication issued shortly after meetings of standard setters, including IFRIC and the EITF, to provide timely feedback on issues discussed at the meeting. We will continue to share all relevant updates with you.
Independence standards	PwC has policies and systems designed to comply with relevant independence and client retention standards. Before a piece of work can begin for the Group, it must first be authorised by Andrew Paynter who evaluates the project against our own internal policies and safeguards. We will report to the Audit and Risk Committee any independence issues as they arise and present an annual summary at the Audit and Risk Committee meeting in June.
Ethics	Our Ethics and Business Conduct Programme includes confidential communication channels to voice questions and concerns 24 hours a day, seven days a week. Confidentiality helps us to ensure that we receive candid information and that we respond with the appropriate technical and risk management resources.

Confirmation of independence

We confirm that in our professional judgement, as at the date of this report, we comply with UK regulatory and professional requirements, including the Ethical Standard issued by the Auditing Practices Board and our objectivity is not compromised.

A letter will be issued to the Audit and Risk Committee in June 2020 to formally confirm our independence.

POL00423684

Appendix 3 - Risk of fraud

International Standards on Auditing state that we as auditors are responsible for obtaining reasonable assurance that the financial statements taken as a whole are free from material misstatement, whether caused by fraud or error. The respective responsibilities of auditors, management and those charged with governance are summarised below:

Auditors' responsibility

Our objectives are:

- to identify and assess the risks of material misstatement of the financial statements due to fraud;
- to obtain sufficient appropriate audit evidence regarding the assessed risks of material misstatement due to fraud, through designing and implementing appropriate responses; and
- to respond appropriately to fraud or suspected fraud identified during the audit.

Management's responsibility

Management's responsibilities in relation to fraud are:

- to design and implement programmes and controls to prevent, deter and detect fraud;
- to ensure that the entity's culture and environment promote ethical behaviour; and
- to perform a risk assessment that specifically includes the risk of fraud addressing incentives and pressures, opportunities, and attitudes and rationalisation.

Responsibility of those charged with governance / the Audit and Risk Committee

Your responsibility as part of your governance role is to evaluate management's identification of fraud risk, implementation of anti fraud measures and creation of appropriate "tone at the top" and to investigate any alleged or suspected instances of fraud brought to your attention.



Your views on fraud

We have had various discussions with management regarding their views on fraud, however we value the Audit and Risk Committee's input and perspective:

- Whether you have knowledge of fraud, actual, suspected or alleged, including those involving management?
- Whether there have been any changes to the measures within Post Office to detect or prevent fraud?
- What role you have in relation to fraud?
- What protocols / procedures have been established between those charged with governance and management to keep you informed of instances of fraud, actual, suspected or alleged?

POL00423684

Appendix 4 – Risk strategy and audit approach summary

FSLI	Inherent	Expected controls reliance	Planned substantive
Fraud risk	Significant	None	High
Going concern	Significant	None	High
Related party transactions	Normal	None	Low
FV of Payzone assets	Normal	None	Low
Postmaster litigation	Significant	None	High
Derivatives	Normal	None	Low
Cash and cash equivalents	Normal	Partial	Low
Property, plant and equipment	Normal	None	Low
Impairment of fixed assets	Significant	None	High
First year adoption of IFRS 16	Elevated	None	Medium
Accounts receivable	Normal	None	Low
Prepaid expenses and other debtors	Normal	None	Low
Inventory	Normal	Partial	Low
Investments in subsidiaries	Normal	None	High
Goodwill	Elevated	None	Medium
Intangible assets subject to amortisation	Elevated	None	Medium
Impairment of intangible assets subject to amortisation	Significant	None	High
Intercompany accounts	Normal	None	Low
Accounts payable	Normal	None	Low
Accruals, provisions and other liabilities	Normal	None	Low
VAT accounting	Elevated	None	Medium
Income taxes	Normal	None	Low
Notes payable and long-term debt	Normal	None	Low
Pension, post retirement and other benefits	Elevated	None	Medium
Share capital and other equity accounts	Normal	None	Low
Revenue	Significant	Partial	High
Cost of sales	Normal	Nonel	Low
Depreciation expense	Normal	None	Low
Operating expenses	Normal	None	Low
Salaries/payroll expense	Normal	Partial	Low
Amortization expense	Normal	None	Low
Trading profit	Elevated	None	Medium
Interest expense	Normal	None	Low
Financial statement preparation and disclosures	Normal	None	Low
Consolidation	Normal	None	Low

POL00423684

Appendix 4 – Risk strategy and audit approach summary (continued)

Fraud in Revenue Recognition

Revenue type	Our assessment and planned response	Audit risk assessment 2019/2020
Fixed contractual	This relates to contracts with customers such as Royal Mail, and is a fixed contractual amount which requires no estimate or judgements to be made by management. Thel fraud risk related to this stream is therefore mitigated to an extent since the amounts are factual per the contract and invoices are raised on a regular basis. The risk therefore reside in the posting of fraudulent journals to overstate revenue. • We will use our journal data auditing techniques noted above to identify and test any journals posted to revenue that appear unusual because they do not follow the Group's normal posting characteristics, i.e. credits to revenue with a corresponding debit to receivables.	• **Significant (existence/ occurrence)**
Horizon to Credence	This relates to commission earned on goods and services sold by the Post Office on behalf of other entities (for example lottery tickets sold on behalf of Camelot). The summary data of the transactions recorded in Credence is transferred into a manually maintained spreadsheet used to calculate commission due from Post Office customers. Invoices are then raised on a monthly basis through CFS which can be individually material. We have rebutted the fraud risk at the consumer transactional level within Horizon, due to the high volume low value nature of the transactions. The fraud risk identified exists at the point where management could introduce fictitious invoices or other journal postings into revenue accounts in the centralised financial reporting process. In addition, there is a risk that revenue may be recognised in the incorrect period to improve reported performance by, for example, incorrectly dating an invoice. Our audit approach to address the risk of fraud in revenue is as follows: • We will use our journal data auditing techniques noted above to identify and test any journals posted to revenue that appear unusual because they do not follow the Group's normal posting characteristics, i.e. credits to revenue with a corresponding debit to receivables. • We will perform detailed testing to high assurance of reconciliations, agreement of commission rates and other third party information to contracts, recalculation of revenue and accrued/deferred income positions and agreeing evidence of cash receipts in the bank, and will also leverage our systems control testing over Horizon. • We will test a sample of revenue transactions recognised pre year end, tracing them back to the Credence summary pre year end to ensure it meets the revenue recognition criteria.	• **Significant (existence/ occurrence, cut off)**

POL00423684

Appendix 4 – Risk strategy and audit approach summary (continued)

Fraud in Revenue Recognition

Revenue type	Our assessment and planned response	Audit risk assessment 2019/2020
Direct to CFS	Revenue recognised directly in CFS includes revenue such as Identity and Payment Services, whereby the transactional data from Horizon interfaces directly into CFS through the Agent Billing module. We have rebutted the fraud risk at the consumer transactional level within Horizon due to the high volume low value nature of the transactions. As for the Horizon to Credence revenue stream he fraud risk therefore exists at the point where management could introduce fictitious invoices or other journal postings into revenue accounts in the centralised financial reporting process. In addition, there is a risk that revenue may be recognised in the incorrect period to improve reported performance. • We will use our journal data auditing techniques noted above to identify and test any journals posted to revenue that appear unusual because they do not follow the Group's normal posting characteristics, i.e. credits to revenue with a corresponding debit to receivables. • We will perform detailed testing of reconciliations, agreement of commission rates and other third party information to contracts, recalculation of revenue and accrued/deferred income positions, agreeing evidence of cash receipt in bank to high assurance and leverage our systems control testing over Horizon. • The work performed in relation to ITGCs for Horizon, and the interfaces from Horizon into Agent Billing will provide comfort that revenue has been recognised within the correct period.	• **Significant (existence/ occurrence, cut off)**
Reliance on third parties	Post Office recognise some of their commission revenue based on the amounts communicated to them by the third parties whose products they are selling such as Bank of Ireland, Moneygram and FRES. The third party takes the sales data from the Post Office and calculates the commission owed. The fraud risk relating to this stream is consistent with the stream above whereby we have rebutted the fraud risk at the consumer transactional level within Horizon, due to the high volume low value nature of the transactions. The audit approach for this stream is also consistent with the above, with the exception of cut off testing. For this, we will trace a sample of invoices raised pre year end to supporting documentation from the third party, evidencing when the original transaction with the consumers occurred.	• **Significant (existence/ occurrence, cut off)**
Telecoms	Post Office's telecoms revenue relates to Post Office branded broadband and home phone services provided to customers through the network access providers, TalkTalk and BT. Fujitsu is engaged as a third party organisation, which provides the Post Office with administrative services relating to its telecommunications business (initiating, recording and processing transactions as agent of the entity). As with the other revenue streams, we have rebutted the fraud risk at the transactional level. The risk therefore relates to fraudulent journals being posted to improve revenue. • We will use our aforementioned journal data auditing techniques to identify and test any journals posted to revenue that appear unusual because they do not follow the Group's normal posting characteristics, i.e. credits to revenue with a corresponding debit to receivables.	• **Significant (existence/ occurrence)**

POL00423684

Appendix 5 – Key communications

Under ISA 260, we are required to make a number of specific communications to the Audit and Risk Committee. These communications, the expected timing and details of how they are addressed are summarised in the table below.

	Planning	Completion	As required
Copy of the engagement letter to those charged with governance	✓		
Independence and objectivity confirmation	✓	✓	
Details of non-audit work performed by PwC and the related fees	✓	✓	
Nature and scope of work together with timing of expected reports and results	✓		✓
Changes to the proposed audit plan (including risk assessment)		✓	✓
Expected modifications to the auditors' report		✓	
Uncorrected misstatements		✓	
Significant deficiencies in internal control identified during the audit		✓	
Views about the qualitative aspects of the entity's accounting practices and financial reporting		✓	✓
Matters specifically required by other ISAs to be communicated to those charged with governance		✓	
Final draft of the representation letter		✓	
Any other audit matters of governance interest	✓		✓
Level of agreed audit fees	✓		
Materiality level	✓	✓	

POL00423684

Appendix 6 – Governance reform and related reporting changes

The below guidance is applicable to Post Office Limited for the 2019/2020 year end.

Summary of requirements	Applicable to	Date applicable	Where to report	Links to further guidance
The Companies (Miscellaneous Reporting) Regulations 2018				
Section 172 (1) statement A statement which describes how the directors have had regard to the matters set out in section 172(1)(a) to (f) when performing their duty under section 172.	A company' that is 'large' under the Companies Act 2006, so exceeds two of the following three thresholds (subject to smoothing arrangements where circumstances change): £36 million turnover; £18 million total balance sheet assets; 250 employees).	Periods beginning on or after 1 January 2019.	Strategic report. Unquoted companies must also make the statement available on a website that is maintained by or on behalf of the company, and identifies the company in question.	Companies Act 2006, Section 172 The Companies (Miscellaneous Reporting) Regulations 2018 Corporate Governance: The Companies (Miscellaneous Reporting) Regulations 2018 - Q&A, June 2018 PwC Guidance: New Companies Act reporting regulations for 2019 PwC Guidance: Navigating the stakeholder agenda: Tackling the reporting challenge
Stakeholder engagement Engagement with employees A statement describing employee engagement. The Regulations build on the existing Companies Act disclosure requirements on employees and are relatively detailed and prescriptive in this area. BEIS has been clear that this reporting is not intended to include only information that is strategically material.	A company with over 250 UK employees.	Periods beginning on or after 1 January 2019.	Directors' report. (There is no requirement for this to be made available on a website)	The Companies (Miscellaneous Reporting) Regulations 2018 Corporate Governance: The Companies (Miscellaneous Reporting) Regulations 2018 - Q&A, June 2018 ICSA Guidance: The Stakeholder Voice in Board Decision Making PwC Guidance: New Companies Act reporting regulations for 2019 PwC Guidance: Navigating the stakeholder agenda: Tackling the reporting challenge
Stakeholder engagement Engagement with other stakeholders. A statement summarising "how the directors have had regard to the need to foster the company's business relationships with suppliers, customers and others, and the effect of that regard, including on the principal decisions taken by the company during the financial year". BEIS has been clear that this reporting is not intended to include only information that is strategically material.	A company that exceeds two of the following three thresholds (subject to smoothing arrangements where circumstances change): £36 million turnover; £18 million total balance sheet assets; 250 employees.	Periods beginning on or after 1 January 2019.	Directors' report. (There is no requirement for this to be made available on a website).	

POL00423684

Appendix 6 – Governance reform and related reporting changes (continued)

Summary of requirements	Applicable to	Date applicable	Where to report	Links to further guidance
The Companies (Miscellaneous Reporting) Regulations 2018				
Statement of private company governance arrangements A 'statement of corporate governance arrangements' which includes the following: which governance code has been applied, if any (or what other arrangements are in place); how the chosen code was applied; and any departures from it. Note: a coalition group under the chairmanship of James Wates has been developing a set of governance principles that companies could use for the purposes of the Regulations. It is also intended that other companies could adopt (and report against) the Wates principles voluntarily. The Wates principles are due to be finalised by December 2018.	A company with EITHER: a) 2,000 or more global employees; OR: b) a turnover over £200 million globally and a balance sheet over £2 billion globally. BEIS has been clear that large subsidiary businesses are expected to provide this new reporting, including the major UK operating subsidiaries of a number of international groups.	Periods beginning on or after 1 January 2019.	Directors' report. Unquoted companies must also make the statement available on a website that is maintained by or on behalf of the company, and identifies the company in question.	The Companies (Miscellaneous Reporting) Regulations 2018 Corporate Governance: The Companies (Miscellaneous Reporting) Regulations 2018 - Q&A, June 2018 PwC Guidance: New Companies Act reporting regulations for 2019 FRC, The Wates Corporate Governance Principles for Large Private Companies, June 2018 PwC Guidance: Summary of Wates principles
Revised FRC guidance on the Strategic Report				
Revised Guidance to reflect new regulations and developments The update to the Guidance has focused on: • incorporating the new requirements introduced by the Non-financial reporting Regulations and the section 172 reporting legislation; • strengthening the link between section 172 and the strategic report; and • reflecting changes in practice and other developments which had occurred since the 2014 Guidance was published. The Guidance has persuasive rather than mandatory force, so companies do not need to follow it or explain where they have not done so. The FRC does expect companies to have regard to it where applicable, however	All companies preparing a strategic report.	Available now although some of the Guidance focuses on requirements that apply for periods beginning on or after 1 January 2019.	Strategic report	FRC Revised Guidance on the Strategic Report PwC Guidance: FRC publishes revised Guidance on the Strategic Report PwC Guidance: Navigating the stakeholder agenda: Tackling the reporting challenge

POL00423684

Appendix 6 – Governance reform and related reporting changes (continued)

Summary of requirements	Applicable to	Date applicable	Where to report	Links to further guidance
Revised alternative performance measures (APMs) guidance				
Performance metrics Principles and Practice issued by the FRC APMs remain a focus of the FRC and they have issued recent guidance stating that they will continue to challenge disclosure where there is apparent failure to comply with ESMA's Guidelines, which, in the FRC's view, codify best practice reporting. The report outlines five principles for reporting. • aligned to strategy; • transparent; • in context; • reliable; and • consistent The five principles were designed to consolidate the views of a range of investors to help companies decide how best to present the metrics they want investors to understand and utilise.	The FRC expects compliance by all companies who choose to disclose such metrics when explaining and highlighting various aspects of their historic performance.	Updated guidance was issued in November 2018.	Throughout the Annual Report.	The Lab report 'Performance metrics - Principles and Practice'

POL00423684

Appendix 6 – Governance reform and related reporting changes (continued)

Summary of requirements	Applicable to	Date applicable	Where to report	Links to further guidance
Developments in corporate reporting				
Streamlined Energy and Carbon Reporting (SECR) The Department of Business, Energy and Industrial Strategy (BEIS) have implemented new requirements with regards to energy and carbon reporting. This includes, as a minimum: · UK energy use (to include as a minimum electricity, gas and transport); · Associated Scope 1 (from natural gas and fuel use from transport) and Scope 2 (from electricity) greenhouse gas emissions; · At least one intensity ratio (comparing emissions data with an appropriate business metric – i.e. tonnes of CO_2e per total £m sales revenue); · Information about energy efficiency action taken in the organisation's financial year; · Methodologies used in the calculation of disclosures; and · Previous year's figures for energy use and GHG emissions (not in the first year). Reporting of this sort requires actions to be taken at the beginning of the impacted financial year in order to define the boundaries and scope of reporting, identify the relevant emissions sources within the group, and establish suitable data collection mechanisms, such that accurate year end reporting can be performed.	All large UK companies will be required to disclose energy and carbon reporting. A 'large' company is defined by the Companies Act 2006 as meeting two of the three thresholds: · 250 employees; · £36 million revenue; and / or · £18 million balance sheet total	For financial years beginning from 1 April 2019 onwards (Applicable to Post Office Limited for the year ending 31 March 2020)	All 'large' UK companies will be required to disclose energy and carbon information within their accounts and reports.	PwC Guidance: Are you ready? Streamlined Energy & Carbon Reporting (SECR) Environmental Reporting Guidelines: Including streamlined energy and carbon reporting guidance

POL00423684

Appendix 7 – Component team reporting timetable

Consistent with 2018/2019, we have engaged with KPMG LLP, the auditors of Bank of Ireland and First Rate Exchange Services Holding Limited ("FRESH"), to report to us on Post Office's share of FRESH's profit for 2019/2020. To obtain sufficient audit evidence over Post Office's 50% profit share, we are instructing KPMG LLP to perform a full scope audit of FRESH for the year ending 29 March 2020.

We have included our expected reporting timetable for the audit of FRESH below.

Deliverable/event	Due date
Planning meeting with component teams	December 2019
Issue group instructions to component teams	January 2020
Component teams to issue acknowledgement of receipt, independence confirmation and early warning memorandum	February 2020
Component teams to issue inter-office/inter-firm opinion and memorandum of work performed	May 2019
Review of component team working papers	May 2019
Subsequent events procedures	June 2019

POL00423684

We have prepared this report solely for the use of Post Office Limited. This report forms part of the continuing dialogue between the company and us and therefore it is not intended to include every matter, whether large or small, that has come to our attention, through our audit. For this reason, this report should not be made available to third parties, and if any third party were to obtain a copy without prior written consent, we would not accept any responsibility for any reliance that they might place on it.

© 2019 PricewaterhouseCoopers LLP. All rights reserved. In this document, "PwC" refers to the UK member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.

POL00423684

Author: David Parry

Meeting date: 25 November 2019

ARC Meeting Dates 2020-2021

Context

The Committee is requested to note the future meetings dates scheduled in respect of the Audit, Risk and Compliance Committee for 2020-2021.

Please note, an additional Committee meeting will be held in June via telephone to discuss the ARA. Date to be confirmed.

The Report

2020

Date			Time	Meeting
Tuesday	28 January	2020	09.30 – 12.00	ARC
Tuesday	24 March	2020	09.00 – 11.30	ARC
Tuesday	19 May	2020	09.30 – 12.00	ARC
Monday	27 July	2020	14.30 – 17.00	ARC
Tuesday	22 September	2020	09.00 – 11.30	ARC
Tuesday	24 November	2020	09.00 – 11.30	ARC

2021

Date			Time	Meeting
Tuesday	26 January	2021	09.00 – 11.30	ARC
Tuesday	30 March	2021	09.00 – 11.30	ARC

14

Strictly Confidential